Tomi Lätti

PK-yrityksen ensimmäisen palvelimen suunnittelu

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikka
Insinöörityö
22.11.2011

Metropolia

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Tomi Lätti PK-yrityksen ensimmäisen palvelimen suunnittelu 52 sivua 22.11.2011
Tutkinto	Insinööri
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Janne Salonen Toimitusjohtaja Antti Immonen

Insinöörityön tarkoituksena oli suunnitella ARANT OY:lle sellainen palvelinlaitteisto ja –ohjelmisto, joka tulisi korvaamaan verkkolevyn yrityksen tiedostojen säilytyspaikkana. Palvelimen ensisijaiset tavoitteet olivat tarjota web-pohjaista verkkolevyä käytännöllisempi tallennustila yrityksen tiedostoille, suorittaa laskutusohjelmistoa palvelimella ja mahdollistaa näiden käyttö etäyhteydellä internetin yli.

Insinöörityössä tutkittiin erilaisia palvelinlaitteistoja ja niihin liittyviä teknologioita, jotta kohdeyritykselle osattaisiin suunnitella ja valita sopiva palvelinlaitteisto. Palvelinlaitteiston vaihtoehtoja tutkittiin eri kotelotyypeistä lähtien yksittäisiin komponentteihin asti ja selvitettiin niiden eroja työasematietokoneiden toteutuksiin.

Palvelimen käyttöjärjestelmäksi oli valittu jo insinöörityön alkuvaiheessa Windows Server 2008, jota tutkittiin sen ominaisuuksien, käyttömahdollisuuksien, käyttöönoton ja hallinnan osalta. Käyttöjärjestelmää tutkittiin erityisesti kohdeyrityksen toteutukselle olennaisten asioiden kannalta, joita olivat tiedostopalvelimena toimiminen sekä etätyöpöytäpalveluiden toiminta ja niiden käyttäminen.

Tehdyn tutkimustyön perusteella hankittiin kohdeyrityksen tarpeisiin soveltuva palvelinlaitteisto, jonka perustana oli Hewlett-Packardin tornipalvelin. Palvelimeen hankittiin erikseen tarvikevalmistajien kiintolevyt ja kiintolevykelkat sekä paikallista hallintaa varten syöttö- ja näyttölaitteet. Lisäksi palvelimeen hankittiin vikasietoisuuden parantamiseksi varavirtalähde ja -tuuletinsarja.

Insinöörityön koostuessa ainoastaan palvelimen suunnittelusta, jäi käyttöjärjestelmän osuus ainoastaan teoriatiedoksi, joka suunniteltiin hyödynnettäväksi myöhemmin palvelimen asennuksen, testauksen ja käyttöönoton yhteydessä.

Avainsanat	Windows Server 2008, palvelin, RAID, DHCP, Remote Desktop

Metropolia

Abstract

Author(s) Title Number of Pages Date	Tomi Lätti Designing First Server for Small or Medium Sized Company 52 pages 22.11.2011
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Janne Salonen, Principal Lecturer Antti Immonen, Managing Director

The goal of this thesis was to design such a server hardware and software to ARANT Ltd, that would replace the company's current online storage space as a repository for its files. The main priorities of the server were to provide a more convenient storage space than the web-based network drive, to run a billing software on the server and to enable its use remotely over the internet.

In the thesis a variety of server hardware and related technologies were studied in order to achieve a knowledge about them enabling to plan a server hardware suitable for the company. The server hardware was studied from different housing types to the properties of individual components and their differences with desktop computer implementations.

The server operating system was selected to be Windows Server 2008 at the very beginning of the study. In the thesis the properties, deployment and management of the operating system were studied in order to be able to implement them later. The operating system was studied specifically as to the properties essential to the company, which were its File Services Role and Remote Desktop Role Service.

The studies carried out resulted in a selected server hardware suitable for the company, and such a knowledge about the operating system that the server can be implemented and managed successfully in due time.

Keywords	Windows Server 2008, server, RAID, DHCP, Remote Desktop

Sisällys

Lyhenteet ja määritelmät

ACE *Access Control Entry*. Käyttöoikeuksia sisältävän listan syöte.

ACL *Access Control List*. Tietoteknisten laitteiden käyttämä lista käyttöoikeuksista.

ARP *Address Resolution Protocol*. Protokolla, jolla Ethernet-verkoissa selvitetään IP-osoitetta vastaava MAC-osoite.

BIOS *Basic Input Output System*. Tietokoneohjelma, jonka suorittamisella tietokoneen käynnistäminen alkaa.

CDFS *Compact Disk File System*. CD-levyjen tiedostojärjestelmä.

CRC *Cyclic Redundancy Check*. Tiedonsiirrossa laajalti käytetty algoritmi, jolla luodaan virheiden havaitsemiseen ja korjaamiseen käytetty tarkisteavain.

DFS *Distributed File System.* Hajautettu tiedostojärjestelmä, joka muodostaa useista eri tiedostosijainneista yhden loogisen näkymän.

ECC *Error-correcting code memory*. Tietokoneiden muistikammoissa käytetty virheenkorjaustekniikka.

EFS *Encrypting File System*. Windows-käyttöjärjestelmien tukema tiedostojärjestelmän salaustekniikka.

Ethernet Yleisin pakettipohjainen lähiverkkoratkaisu.

FAT *File Allocation Table*. Laajalti tuettu, nykyisin muistitikuissa käytetty tiedostojärjestelmä.

GPT *GUID Partition Table*. Tietokoneiden tallennuslaitteissa käytetty osiointitapa.

HTTPS *Hypertext Transfer Protocol Secure*. Salattu versio HTTP-protokollasta, jota internet-selaimet ja web-palvelimet käyttävät tiedonsiirtoon.

IEC *International Electrotechnical Commission*. Kansainvälinen sähköalan standardoimisjärjestö.

IEEE *Institute of Electrical and Electronics Engineers*. Kansainvälinen tekniikan alan järjestö, joka määrittelee alan keskeisiä standardeja.

IIS *Internet Information Services*. Microsoftin web-palvelinohjelmisto.

iSCSI *Internet Small Computer System Interface*. IP-verkossa liikennöivä versio SCSI:stä.

ISO *International Organization for Standardization*. Kansainvälinen standardoimisjärjestö.

LFF *Large Form Factor*. Tietotekniikan kokoluokkanimitys, jota käytetään useiden laitteiden normaalikokoisista malleista.

LPR *Line Printer Remote.* Verkkoprotokolla, joka mahdollistaa tulostustöiden lähettämisen verkon yli.

MAC *Media Access Control*. IEEE 802 –verkoissa (esimerkiksi Ethernet) varaamisen ja liikennöinnin hoitava osajärjestelmä.

MBR *Master Boot Record*. Tietokoneiden tallennuslaitteissa käytetty osiointitapa.

NAS *Network Attached Storage*. Tietoverkkoon liitetty tallennuslaite.

NAT *Network address translation*. Osoitteenmuunnostekniikka, jota käytetään IP-osoitteiden tehokkaampaan hyödyntämiseen.

NBD *Next Business Day*. Seuraava työpäivä, eli aikamääre. Käytössä usein on-site takuun yhteydessä.

NFS *Network File System.* Hajautetun tiedostojärjestelmän protokolla, joka mahdollistaa tiedostojen käytön verkon yli.

NTFS *New Technology File System*. Microsoftin kehittämä tiedostojärjestelmä, joka on käytössä Microsoft Windows NT -pohjaisissa käyttöjärjestelmissä.

RD *Remote Desktop*. Etätyöpöytä, jonka avulla tietokonetta voidaan käyttää etäyhteydellä toiselta tietokoneelta.

RDC *Remote Desktop Connection*. Etätyöpöytäyhteys, joka luodaan kahden tietokoneen välille.

RDP *Remote Desktop Protocol*. Microsoftin kehittämä ja omistama protokolla, joka mahdollistaa etätyöpöytäyhteydet Windows-tietokoneiden välillä.

RPM *Rotations Per Minute*. Suure, joka ilmoittaa, montako kierrosta kappale pyörähtää akselinsa ympäri tietyssä ajassa.

SAN *Storage Area Network*. Tallennuslaitteille varattu tietoverkko tai sen osa.

SAS *Serial Attached SCSI*. Sarjamuotoinen versio SCSI:stä.

SATA *Serial Advanced Technology Attachment.* Tietotekniikassa käytetty sarjamuotoinen massamuistilaitteiden liitäntä.

SCSI *Small Computer System Interface*. Standardi tiedon välittämiseksi tietokoneen ja oheislaitteiden välillä.

SFF *Small Form Factor*. Tietotekniikan kokoluokkanimitys, jota käytetään useiden laitteiden tilaa säästävistä malleista.

SSD *Solid State Drive*. Tietokoneen kiintolevymalli, jossa tieto tallennetaan muistipiireille.

Tavu Digitaalisen tiedon mittayksikkö, jota käytetään tietotekniikassa useimmiten SI-järjestelmän kymmenkantaisilla kerrannaisyksiköillä. Tavun oikeaoppiset monikerrat ovat kuitenkin tässäkin työssä käytetyt binäärijärjestelmän kahden potenssit. [1].

TCP/IP *Transmission Control Protocol / Internet Protocol*. Usean tietoverkkoprotokollan yhdistelmä, jolla huolehditaan verkon laitteiden osoitteista ja pakettien reitittämisestä.

TPM *Trusted Platform Module*. Spesifikaatio kryptosuorittimelle, joka tallentaa salausavaimia.

UDF *Universal Disk Format*. DVD-levyjen tiedostojärjestelmä.

VHD *Virtual Hard Disk*. Virtuaalinen tiedostojärjestelmä, jolle on tuki useassa Windows-käyttöjärjestelmässä.

VPN *Virtual Private Network*. Tekniikka, jolla voidaan muodostaa julkisen verkon yli näennäisesti yksityinen yhteys.

WSUS *Windows Server Update Services*. Windows Server –käyttöjärjestelmän palvelinrooli, joka lataa ja jakaa päivityksiä Windows-käyttöjärjestelmille.

1 Johdanto

Insinöörityön tavoitteena on suunnitella ARANT OY:lle palvelinratkaisu, joka tulee korvaamaan yrityksen vanhan web-pohjaisen verkkotallennustilan. Palvelimen ensisijaisena tarkoituksena on tarjota käytettävyydeltään verkkolevyä parempi tallennustila yrityksen tiedostoille sekä mahdollistaa laskutusohjelmiston suorittaminen palvelimella. Palvelimen on tarkoitus mahdollistaa sekä tiedostojen että laskutusohjelmiston etäkäyttö internetin kautta.

Tavoitteiden mukainen palvelinratkaisu helpottaa ja yksinkertaistaa yrityksen tiedostojen keskitettyä säilyttämistä, käyttöä ja hallintaa. Myös laskutusohjelmiston suorittaminen keskitetysti palvelimella yksinkertaistaa sen käyttöä usean henkilön toimesta. Palvelin tarjoaa yritykselle myös uusia mahdollisuuksia, kuten web-palvelimena toimimisen yrityksen mahdollisille internet-sivuille.

Insinöörityössä tutkitaan erilaisia palvelinlaitteistoja, käyttöjärjestelmän ominaisuuksia ja näiden luomia käyttömahdollisuuksia. Näiden tietojen perusteella valitaan kohdeyritykselle palvelinlaitteisto ja –ohjelmisto. Insinöörityössä käsiteltävä teoriatieto palvelinlaitteiston ja käyttöjärjestelmän osalta on sellaista, joka on kohdeyrityksen toteutuksen kannalta oleellista.

2 Insinöörityön kohdeyritys

2.1 Yrityksen kuvaus

ARANT OY on vuonna 2008 perustettu automaatio- ja sähköalan yritys, joka työllistää tällä hetkellä 5 henkilöä. Yritys tekee alansa asennus- ja suunnittelutöitä, markkina-alueenaan koko Suomi. Yrityksen nykyiset tilat sijaitsevat Sulan teollisuusalueella Tuusulassa. Yritys on muuttamassa vuoden vaihteessa 2011-2012 isompiin tiloihin samalle alueelle.

Yrityksen tärkeimpiä asiakkaita ovat Arla Ingman Oy ja Industri Textil Job Oy. Yritys tekee Arla Ingmanin elintarviketehtaalla mm. prosessiautomaation kunnossapito-,

asennus- ja suunnittelutöitä sekä projektointia. Industri Textil Jobille yritys tekee suodatinjärjestelmien ohjauskeskuksien suunnittelua, kokoonpanoa ja asennustyötä.

2.2 Insinöörityön lähtökohdat

Yrityksen toiminnassa syntyy runsaasti erilaisia tiedostoja, joiden säilöminen vaatii digitaalista tallennustilaa. Tiedostoja syntyy normaalin liiketoiminnan asiakirjojen lisäksi yrityksen tekemistä töistä, esimerkiksi koestuspöytäkirjojen ja automaatiosuunnittelun piirrosten muodossa. Tiedostot halutaan säilyttää keskitetysti yhdessä toimintavarmassa paikassa, jossa ne ovat helposti käytettävissä.

Vanha toteutus

Yrityksen tähänastinen toteutus tiedostojen tallentamiseen on internetoperaattori Elisalta hankittu verkkolevypalvelu. Verkkolevy on määrätyn kokoinen tallennustila operaattorin palvelimilla. Verkkolevyä käytetään web-selaimella sille varatussa internet-osoitteessa. Verkkolevyn ongelmana on kuitenkin web-käyttöliittymän aiheuttama rajoittunut käytettävyys. Tiedostojen käsittely on ongelmallista seuraavista syistä:

- Verkkolevyn käyttö vaatii mielellään nopean internetyhteyden.
- Verkkolevyn käyttö on mahdollista vain web-selaimella.
- Vain yhden tiedoston voi lisätä kerrallaan.
- Tiedostoa ei voi muokata verkkolevyllä, vaan se pitää ensin ladata tietokoneelle muokattavaksi ja sen jälkeen siirtää takaisin verkkolevylle.

Vaatimukset ja tavoitteet

Palvelin tulee korvaamaan vanhan verkkolevytoteutuksen kokonaan, joten palvelimelle tullaan tallentamaan kaikki yrityksen sähköiset asiakirjat ja piirrokset. Lisäksi palvelimelle tullaan asentamaan ainakin yrityksen laskutusohjelmisto. Tiedostojen ja laskutusohjelmiston tulee olla käytettävissä etäyhteydellä internetin kautta. Näistä syistä johtuen palvelimen tulee olla toimintavarma, vikasietoinen ja tietoturvallinen.

Palvelinlaitteistoksi tulee valita sellainen kokonaisuus, jonka tehokkuus ja ominaisuudet riittävät suunnitelluille toiminnoille ja mahdollisille tulevaisuuden lisätoiminnoille.

Palvelinlaitteiston suunnittelussa tulee varautua sen mekaanisesti vikaherkimpien osien, kuten kiintolevyn ja virtalähteen rikkoutumisiin. Palvelimen tulee säilyä toimintakuntoisena esimerkiksi yhden kiintolevyn rikkoutumisesta huolimatta.

Palvelimelle tulee varata tarpeeksi tallennuskapasiteettia, jotta uusille tiedostoille riittää tilaa ja vanhoja voidaan säilyttää useita vuosia. Tiedostot tulee myös varmuuskopioida ulkoiselle medialle, kuten erilliselle kiintolevylle. Varmuuskopioinnin on tapahduttava automaattisesti säännöllisin väliajoin.

Palvelinkäyttöjärjestelmäksi tulee valita sellainen tuote, joka on toimintavarma, tietoturvallinen ja yhteensopiva valitun palvelinlaitteiston kanssa. Käyttöjärjestelmän tulee olla graafisella käyttöliittymällä varustettu ja sen tulee olla tarpeeksi selkeä ja helppokäyttöinen sellaisen henkilön opittavaksi, joka ei tunne palvelinkäyttöjärjestelmiä. Käyttöjärjestelmän tulee mahdollistaa käyttäjätilien oikeuksien määrittäminen, jotta käyttäjien pääsyä tiedostoihin voidaan rajoittaa.

Tiedostojen ja ohjelmistojen etäkäytön mahdollistamiseksi palvelin tullaan liittämään internetiin. Tästä syystä etäkäyttöyhteydet tulee määrittää salatuiksi ja tietoturvallisiksi. Etäkäyttöyhteyksien tulee kuitenkin olla helppokäyttöisiä ja vaivattomia. Palvelinkäyttöjärjestelmän ja tiedostojen tietoturvallisuudesta tulee huolehtia palomuurin, virustorjunnan ja ohjelmistopäivitysten avulla. Käyttöjärjestelmän ja virustorjuntaohjelmiston päivitysten tulee tapahtua automaattisesti ylläpitotoimien vähentämiseksi.

Palvelinlaitteiston ja -käyttöjärjestelmän suunnittelussa tulee myös ottaa huomioon mahdollinen lisätoiminnallisuuksien tarve tulevaisuudessa. Tällaisia lisätoiminnallisuuksia ovat esimerkiksi seuraavat:

- tulostinpalvelin
- web-palvelin yrityksen kotisivuja varten
- DHCP-palvelin yrityksen toimitilojen laitteille
- WSUS-palvelin yrityksen toimitilojen Windows-tietokoneille.

Nämä toiminnallisuudet esitellään tarkemmin luvussa 5.

Suunniteltava palvelinratkaisu tullaan sijoittamaan toimitiloihin, joihin kohdeyritys muuttaa vuoden vaihteessa 2011-2012. Tästä johtuen palvelimen asennus, testaus ja käyttöönotto siirtyvät ensi vuodelle, eikä niitä käsitellä tässä insinöörityöraportissa.

3 Laitteisto

3.1 Kotelotyypit

Tornipalvelin

Tornipalvelin tarkoittaa sellaista palvelinta, jossa palvelimen osat on asennettu pöytätietokonetta muistuttavaan tornikoteloon. Tornikotelon suhteellisen suuri fyysinen koko tarjoaa usein muita kotelotyyppejä enemmän tilaa ja siten enemmän laajennusmahdollisuuksia. Tornipalvelimia säilytetään yleensä sellaisinaan esimerkiksi lattialla, mutta tarjolla on myös tornikoteloita, jotka voidaan asentaa palvelinräkkiin. Kokonsa vaatiman tilan takia tornipalvelin on kuitenkin järkevä valinta vain silloin, kun samaan paikkaan sijoitettavia palvelimia ei tarvita montaa kappaletta.

Räkkipalvelin

Räkkipalvelimissa palvelimen osat on sijoitettu tornipalvelinta pienempään, litteän malliseen koteloon, jonka koko on standardin mukainen. Räkkipalvelimet asennetaan räkeiksi kutsuttuihin laitetelineisiin tai -kaappeihin. Pienen kokonsa ansiosta räkkipalvelin on huomattavasti tornipalvelinta järkevämpi vaihtoehto silloin, kun palvelimia tarvitaan useita. Standardikokoisiin räkkeihin on tarjolla myös paljon muuta kuin palvelinlaitteistoa, mikä voi tilanteesta riippuen tehdä räkkipalvelimesta tornipalvelinta järkevämmän vaihtoehdon. Esimerkki räkkipalvelimista on kuvassa 1.

Kuva 1. Räkkipalvelimia laitekaapissa [2].

Blade-palvelin

Blade-palvelin on laiteräkkiin asennettava kokonaisuus, joka käsittää erillisen rungon ja siihen asennettavat palvelinkortit. Blade-palvelimen ideana on minimoida fyysisen tilan ja energian käyttö keskittämällä virransyöttö, jäähdytys, verkkotoiminta ja palvelinkorttien hallinta erilliseen runkoon. Tämän ansiosta jokainen palvelinkortti ei tarvitse esimerkiksi omaa virtalähdettä, mikä säästää tilaa, energiaa ja kustannuksia.

Blade-palvelimen rungon hoitaessa palvelimen ylläpidon, suorittavat palvelinkortit vain varsinaisia palvelintoimintoja, kuten tiedostonjakoa ja tai virtualisointia. Blade-palvelin on toteutettu modulaarisella rakenteella, johon voidaan vaihtaa palvelinkortteja jopa käytön aikana. Runkoon asennettavia kortteja on myös muihin tarkoituksiin, kuin palvelinkäyttöön. Tällaisia ovat esimerkiksi verkkolaitteiden, kuten kytkimien, reitittimien ja verkkolevyjen blade-toteutukset. Esimerkki blade-palvelinkokonaisuudesta on kuvassa 2. [3.]

Kuva 2. Blade-palvelinkokonaisuus, jossa on 16 palvelinkorttia ja pohjalla 2 UPS-virtalähdettä [3].

3.2 Komponentit

Palvelimien peruskomponentit ovat samankaltaisia kuin työasematietokoneiden vastaavat. Erilaisista käyttötarkoituksista johtuen eroja kuitenkin on enemmän tai vähemmän, riippuen osa-alueesta. Palvelinkomponentit ovat yleensä korkeampilaatuisia ja siten kalliimpia kuin työasemien vastaavat johtuen palvelinkäytön vaatimuksista esimerkiksi luotettavuuden suhteen. Tässä luvussa ei käsitellä kaikkia komponentteja tai niiden ominaisuuksia yleisesti, vaan huomion arvoisia asioita nimenomaan palvelinkäytön kannalta.

Emolevy

Palvelimien emolevyt sisältävät useasti enemmän muistipaikkoja sekä suoritinkantoja verrattuna työasemiin, joissa on tyypillisesti vain yksi suoritin ja 2-4 muistipaikkaa. Suoritinkannat voivat olla sellaisia, joihin sopii vain palvelinkäyttöön suunnitellut suorittimet. Myös kiintolevyohjaimet ovat työasemien vastaavia monipuolisempia, jos emolevyssä itsessään sellainen on. Koska palvelin yleensä toimii verkossa, on emolevyissä enemmän kuin yksi nopea verkkoliitäntä.

Emolevyissä on usein ominaisuuksiltaan varsin vaatimaton integroitu näytönohjain, koska palvelinkäytössä graafinen prosessointi on vähäistä. Emolevyissä on harvoin äänilaitteistoa. Monesti palvelimilla ei ole näyttöä, näppäimistöä ja hiirtä, koska palvelimia hallitaan etäyhteydellä verkon kautta.

Suoritin

Palvelimen suoritinvaatimukset vaihtelevat käyttötarkoituksen mukaan, sillä esimerkiksi sovelluksien ajaminen kuormittaa suorinta enemmän kuin tiedostojen jakaminen. Monesti samaa palvelinta kuitenkin käytetään useampaan tarkoitukseen ja yleisesti palvelinlaitteistoissa onkin panostettu suorittimen tai suorittimien tehokkuuteen.

Palvelimien suorittimet ovat työasemien tapaan nykyään moniytimisiä, mikä parantaa moniajoa, eli usean prosessin samanaikaista suoritusta. Palvelinkäytössä moniajo on suuressa roolissa, mistä johtuen suorittimia voi olla useita ja yksittäisessä suorittimessa voi olla jopa 12 ydintä. Palvelinsuorittimilla on useammin tuki virheenkorjaavalle ja rekisteröidylle muistille kuin normaalikäyttöön tarkoitetuilla suorittimilla.

Muisti

Muisti on palvelimissa työasemien tapaan suuressa roolissa, koska tietokone käyttää sitä käsiteltävän tiedon tallentamiseen. Palvelimissa käytettävät muistikammat ovat samanlaisia kuin työasemissa sillä erotuksella, että palvelinkäytössä on huomattavasti yleisempää käyttää rekisteröityjä ja virheenkorjaavia muisteja.

Rekisteröity tarkoittaa sellaista muistikampaa, jossa muistipiirejä varten on rekisterit, joihin emolevyn muistiohjain viittaa. Tämä vähentää muistiohjaimen kuormitusta ja lisää järjestelmän vakautta, mutta myös hidastaa muistin toimintaa.

Virheenkorjaava muisti (Error-correcting code memory, ECC) tallentaa erillisiin muistipiireihin pariteettitietoa, jonka avulla voidaan korjata havaittu virhe. Virheenkorjaava muisti vähentää pieniä muistivirheitä, mikä on tarpeellista palvelinkäytössä, jossa luotettavuus on suuressa roolissa.[4; 5.]

3.3 Levyjärjestelmät

3.3.1 Kiintolevytyypit ja liitännät

Nykyään yleisimmät kiintolevyt on jaettu fyysisen kokonsa puolesta kahteen luokkaan, jotka ovat 2,5” ja 3,5”. Tuumakoko tarkoittaa kiintolevyn sisällä pyörivän, yhden tai useamman metalli- tai lasikiekon halkaisijaa. Näistä käytetään myös nimityksiä SFF (Small Form Factor) 2,5 tuumaiselle ja LFF (Large Form Factor) 3,5 tuumaiselle.

Kiintolevyn suorituskyvyn paras mittari on sen kiekon tai kiekkojen pyörimisnopeus. Yleisimmät kiintolevyjen pyörimisnopeudet ovat 5400 rpm (Rotations Per Minute), 7200 rpm ja 10 000 rpm. Vaativimmissa palvelintoteutuksissa on käytössä myös nopeampia kiintolevyjä, joiden pyörimisnopeus on jopa 15 000 rpm. Suuremman pyörimisnopeuden kiintolevyt toimivat nopeammin, mutta ovat myös kalliimpia.

Kiintolevyjen tallennuskapasiteetti kasvaa kehityksen myötä jatkuvasti. Tällä hetkellä suurimmat kapasiteetit ovat muutaman Teratavun luokkaa, mutta myös alle sadan Gigatavun kapasiteetin kiintolevyjä on vielä saatavilla.

Jatkuvasti yleistyvä ja hiljalleen perinteisiä kiintolevyjä korvaava kiintolevytyyppi on SSD (Solid State Drive). SSD-kiintolevyssä ei ole liikkuvia osia, vaan siinä tieto tallennetaan flash-muistipiireille. SSD-kiintolevyn edut palvelinkäytössä perinteisiin verrattuna ovat osittain nopeampi toiminta, pienempi virrankulutus, pienempi lämmöntuotto, pienempi koko ja parempi lämmönkesto. Haittapuolena on korkea hinta tallennuskapasiteettiin nähden. Myös SSD-kiintolevyjen käyttöikää ja luotettavuutta on kyseenalaistettu. [6, s. 214; 7.]

Liitännät

Kiintolevyjen nopeuden ja kapasiteetin kanssa aivan yhtä tärkeä asia on liitäntärajapinta, jolla kiintolevyt yhdistetään muuhun laitteistoon. Palvelimen levynkuormitus voi olla hyvinkin suurta, jolloin hidas liitäntä voi muodostua suorituskyvyn pullonkaulaksi.

Pienemmissä palvelimissa on yleensä työasemien tapaan käytössä SATA-liitäntä (Serial Advanced Technology Attachment). SATA-standardista on tällä hetkellä kolme versiota, joista ensimmäisen siirtonopeus on 1,5 Gbit/s (gigabittiä sekunnissa), toisen 3 Gbit/s ja kolmannen 6 Gbit/s. Näistä 2. versio on tällä hetkellä yleisin, mutta 3. versio yleistyy jatkuvasti. SATA-liitäntä mahdollistaa kiintolevyjen asentamisen ja poistamisen ilman, että tietokonetta tarvitsee sammuttaa. SATA-liitäntä tukee vain yhtä laitetta per liitäntä.

Suuremmissa palvelimissa on yleisesti käytössä SAS-liitäntä (Serial Attached SCSI), joka on yhteensopiva myös SATA-liitäntäisten kiintolevyjen kanssa niiden 2. versiosta eteenpäin. SAS-liitännät nopeudet ovat 3 Gbit/s ja 6 Gbit/s. SAS-liitäntään voidaan laajennuskomponenttien avulla liittää jopa tuhansia kiintolevyjä tai muita laitteita. SAS-liitäntäiset kiintolevyt ovat vastaavia SATA-liitäntäisiä kalliimpia, mutta liitännän etu onkin siinä, että molempia levyjä voidaan käyttää tarpeen mukaan. Tarjolla on myös kiintolevyjä, joissa on liitännät molemmille tekniikoille. [6, s. 214; 8.]

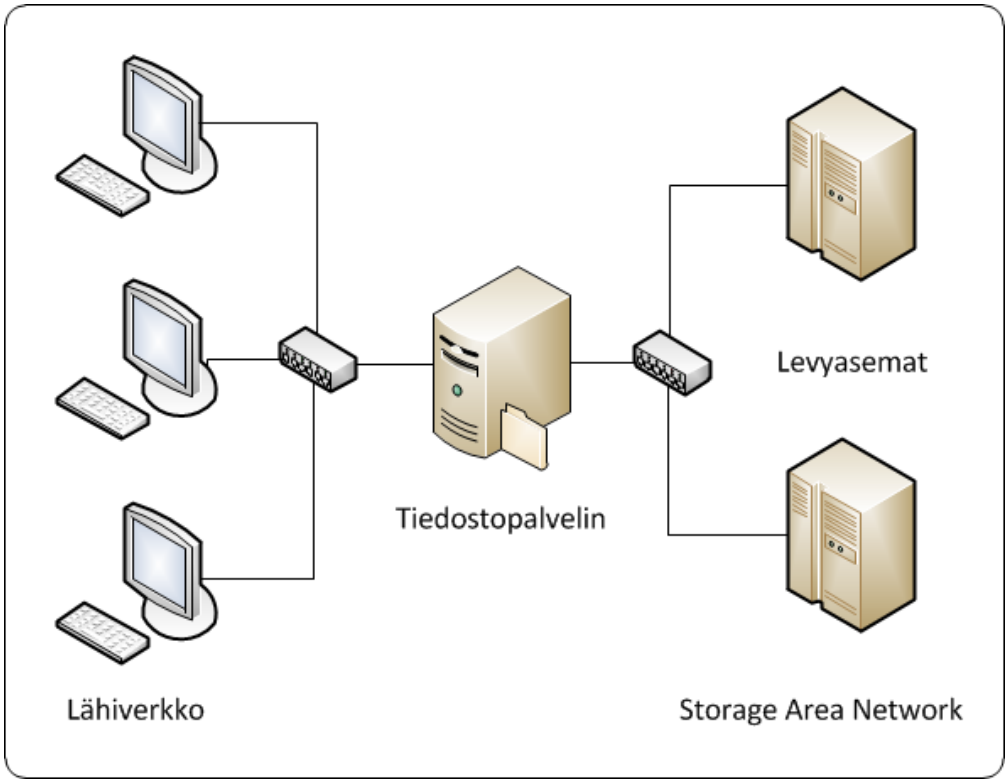
3.3.2 Ulkoiset levyasemat

Suuren tallennuskapasiteetin palvelinlaitteistoissa kiintolevyt ovat yleensä erillisessä levyasemassa, joka tyypillisesti sisältää virtalähteen, jäähdytyksen, levyohjaimen ja erillisen välimuistin. Levyaseman avulla palvelimeen voidaan liittää enemmän kiintolevyjä, kuin palvelimen omaan koteloon mahtuisi. Kiintolevyt ovat kuitenkin samanlaisia, kuin mitä käytetään sisäisinä kiintolevyinä. Usein levyasemat tarjoavat myös vikasietoisuutta parantavia ominaisuuksia, joita on esitelty luvussa 3.4.

Ulkoinen levyasema voidaan liittää tietokoneeseen kiintolevyliitännällä kuten SASilla, oheislaiteliitännällä kuten USB:llä, tai verkkoliitännällä kuten iSCSI (Internet Small Computer System Interface) tai Fibre Channel. Yleensä ulkoiset levyasemat toimivat toisella seuraavista arkkitehtuureista:

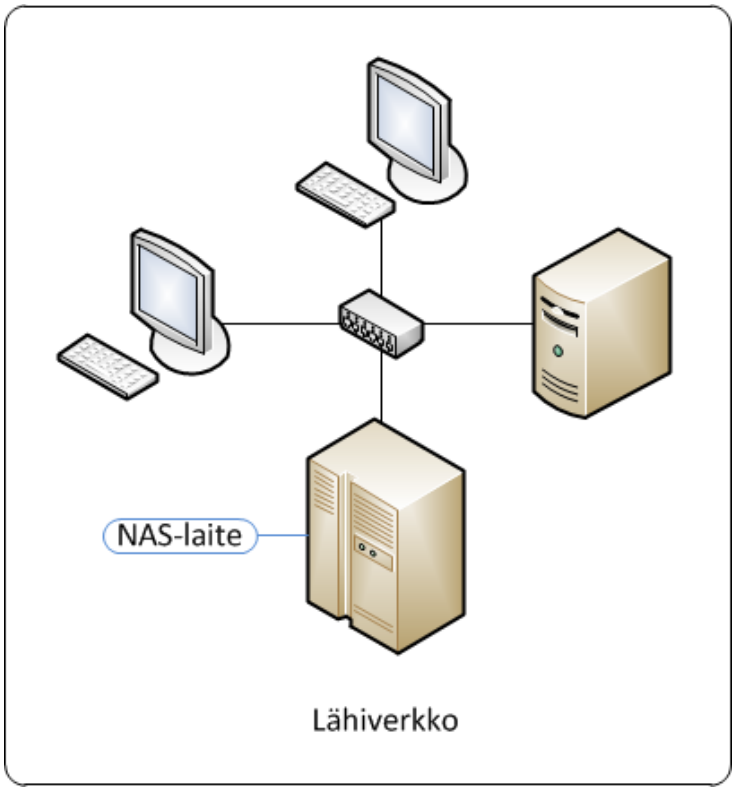
SAN (Storage Area Network) on erillinen verkko, joka on varattu ainoastaan tallennuslaitteille, kuten ulkoisille levyasemille. SAN käyttää nopeaa liitäntätekniikkaa, kuten SCSI:itä tai Fibre Channelia, mikä mahdollistaa suurien tietomäärien siirtämisen

nopeasti. SAN liitetään palvelimeen, joka luo SANin laitteisiin tiedostojärjestelmän ja mahdollistaa niiden käytön normaalista lähiverkosta. SAN liittyy lähiverkkoon kyseisen palvelimen kautta, jolloin palvelimella on erilliset verkkorajapinnat lähiverkolle ja SANille. SANin laitteiden tallennuskapasiteetti näkyy lähiverkon työasemille ja muille laitteille samalla tavalla kuin niiden sisäiset kiintolevytkin. SAN-arkkitehtuuria on havainnollistettu kuvassa 3.



Kuva 3. SAN on erillinen verkko, joka on varattu tallennuslaitteille.

NAS (Network Attached Storage) on tallennuslaite, joka on liitetty suoraan siihen verkkoon, jossa sen asiakaslaitteet sijaitsevat. NAS eroaa SANista pääosin laitteistonsa ohjelmiston osalta. NAS-laitteella on oma suoritin, muistit ym. tarvittavat komponentit, joilla se suorittaa omaa yksinkertaistettua käyttöjärjestelmäänsä. NAS-laite toimii siis kuin tiedostopalvelin, eikä tarvitse muuta laitteistoa toimiakseen. NAS-laite liittyy lähiverkkoon siinä käytettävällä tekniikalla, joka on yleensä Ethernet. NAS-arkkitehtuuria on havainnollistettu kuvassa 4.



Kuva 4. NAS-laite on kytketty suoraan lähiverkkoon ja toimii itsenäisenä tiedostopalvelimena.

NAS on yksinkertainen ja edullinen tapa lisätä tallennustilaa verkon käyttäjille ja vähentää tiedostopalvelimien kuormitusta. NAS-laitteen heikkous on kuitenkin huono tai olematon laajennusmahdollisuus, sillä sen komponentteja ei pääsääntöisesti pysty vaihtamaan. Jos siis NAS-laitteen kuormitus kasvaa liian suureksi, joutuu ostamaan toisen NAS-laitteen. SAN puolestaan käyttää tallennustilan jakamiseen erillistä palvelinta, eli normaalia tietokonelaitteistoa, jota pystyy päivittämään hyvin monipuolisesti. [6, s. 215-216.]

3.3.3 RAID

Redundant Array of Independent Disks (RAID) on tekniikka, jolla kiintolevyt näkyvät yhtenä loogisena levyasemana ja jonka eri variaatioilla kasvatetaan kiintolevyjen vikasietoisuutta, suorituskykyä tai molempia. RAID on hyvin yleisesti käytössä palvelimissa, koska niissä vikasietoisuus ja suorituskyky ovat suuressa roolissa.

RAIDia voidaan käyttää joko ohjelmallisesti esimerkiksi käyttöjärjestelmän toimesta, tai erillisellä RAID-levyohjaimella, jolloin kyseessä on laitetason RAID. Levyohjain voi olla integroituna emolevyyn, erillinen ohjainkortti tai kokonainen ulkoinen levyjärjestelmä.

Useimmiten RAID on toteutettu erillisellä levyohjaimella, koska sen avulla levyn manipulointitoimien ja pariteetin laskennan kuormitus siirtyy tietokoneen suorittimelta itse RAID-ohjaimelle. Pariteetti on matemaattinen algoritmi, jota osa RAID-tasoista käyttää kirjoitusoperaatioissa vikasietoisuuden parantamiseksi.

RAID 0: Lomitus ilman pariteettia.

Tieto tallennetaan lomitettuna tasaisesti kaikille kiintolevyille. Rinnakkaiset luku- ja kirjoitusoperaatiot suoritetaan samanaikaisesti kaikilla kiintolevyillä, mikä parantaa levyjärjestelmän suorituskykyä. Ei vikasietoisuutta eikä virheenkorjausta, joten yhden kiintolevyn rikkoutuminen aiheuttaa kaiken tiedon menettämisen.

Kiintolevyjen vähimmäismäärä on kaksi kappaletta. X kappaletta Y kokoisia kiintolevyjä mahdollistaa X·Y suuruisen tallennustilan ja X-kertaisen luku- ja kirjoitusnopeuden verrattuna yhteen kiintolevyyn. Jos kiintolevyt ovat eri kokoisia, on tallennustilan suuruus X · pienimmän kiintolevyn kapasiteetti.

RAID 1: Peilaus ilman pariteettia.

Tieto tallennetaan samanlaisena jokaiselle kiintolevylle, mikä parantaa levyjärjestelmän lukunopeutta ja vikasietoisuutta. Tiedot ovat tallessa niin kauan, kuin yksikin kiintolevy on toiminnassa.

Kiintolevyjen vähimmäismäärä on kaksi kappaletta. Käytettävä kapasiteetti on aina pienimmän kiintolevyn kapasiteetti, koska kaikkien levyjen täytyy sisältää sama tieto.

RAID 3: Tavutason lomitus erillisellä pariteetilla.

Tieto tallennetaan lomitettuna kaikille paitsi yhdelle kiintolevylle, joka on varattu pariteettitietoa varten. Tieto säilyy yhden kiintolevyn rikkoutuessa, mutta useampien

rikkoutuessa tiedot menetetään. Jokainen kirjoitusoperaatio vaatii kirjoittamisen myös pariteettilevylle, joka tekee siitä suorituskyvyn pullonkaulan. Suorituskyky on kuitenkin hyvin tasainen, ja siirtonopeus kasvaa kiintolevyjen määrän myötä. Kiintolevyjen vähimmäismäärä on kolme kappaletta. RAID 3:n on korvannut laajalti RAID 5, mutta sen toteutuksia on yhä saatavilla.

RAID 4: Lohkotason lomitus erillisellä pariteetilla.

Muuten identtinen RAID 3:n kanssa, mutta RAID 4 käyttää isompia, lohkotason lomituksia, mikä parantaa kiintolevyjen suorituskykyä. Pariteettilevy on tästä huolimatta suorituskyvyn pullonkaula. Myös RAID 4 on korvautunut laajalti RAID 5:llä.

RAID 5: Lomitus hajautetulla pariteetilla.

Tallennettava tieto ja pariteettitieto lomitetaan lohkoina kaikille kiintolevyille, mikä varmistaa, että lohko ja sen pariteettitieto eivät ole ikinä samalla kiintolevyllä. Pariteettitiedon hajauttamisen ansiosta erillistä pariteettilevyä ei tarvita, eikä se siten ole pullonkaulana suorituskyvylle. Pariteettitiedon laskeminen kuitenkin vaatii yhä laskentatehoa. Tieto säilyy yhden kiintolevyn rikkoutuessa.

Kiintolevyjen vähimmäismäärä on kolme kappaletta. X kappaletta Y-kokoisia kiintolevyjä mahdollistaa $X \cdot (Y-1)$ suuruisen tallennustilan, koska yhden kiintolevyn kapasiteetti varataan pariteettitiedon tallentamiseen.

RAID 6: Lomitus hajautetulla tuplapariteetilla.

Muuten identtinen RAID 5:n kanssa, mutta RAID 6 käyttää yhtä ylimääräistä pariteettilohkoa, minkä ansiosta tieto säilyy vielä kahden kiintolevyn rikkoutuessa. [6, s. 217-219; 9; 10.]

3.4 Vikasietoisuus

Vikasietoisuus on useimmiten yksi suurimmista asioista palvelimien suunnittelussa ja toteutuksessa, koska palvelimien sisältämä tieto ja niiden suorittamat toimenpiteet ovat

enemmän tai vähemmän tärkeitä. Esimerkiksi kiintolevyn rikkoutuminen voi aiheuttaa yhdelle organisaatiolle muutaman tunnin menetettyä tuottavuutta, kun taas toiselle organisaatiolle se voi aiheuttaa suuren taloudellisen menetyksen. Sairaalalle potilastietojen menettäminen voi aiheuttaa jopa henkien menettämisen.

Vikasietoisuuden kannalta ratkaiseva asia on välitön redundanssi. Jos yksi kopio tiedostosta menetetään esimerkiksi kiintolevyn rikkoutuessa, korvautuu se välittömästi toisella kopiolla, jolloin tiedosto pysyy käytettävissä. Erilaiset vikasietoisuusmekanismit tarjoavat tällaista redundanssia eri tavoilla. Nämä mekanismit voivat luoda esimerkiksi redundanttisia lohkoja, tiedostoja, kiintolevyjä ja jopa redundanttisia palvelimia.

Monien tietokoneteknologioiden tapaan vikasietoisuus on kompromissi suorituskyvyn ja kustannuksen välillä. Parhaan vikasietoisuuden tarjoava toteutus on yleensä myös kallein. Kiintolevyjen vikasietoisuuden toteutustapa on kompromissi myös tallennuskapasiteetin suhteen.

Laitteiston vikasietoisuus

Palvelimet koostuvat samoista peruskomponenteista kuin työasematkin: suoritin, muisti, kiintolevy, emolevy, virtalähde jne. Palvelinlaitteistojen erot työasemien vastaaviin ovat paitsi yksittäisten komponenttien ominaisuuksien lisäksi se, että tietyt komponentit ovat yleensä kahdennettuja. Kahdennuksella tarkoitetaan toteutusta, jossa on kaksi tai useampia komponentteja toistensa varalla. Kahdennetuilla komponenteilla saavutetaan parempaa suorituskykyä, vikasietoisuutta tai molempia.

Vikasietoisuuden parantamiseksi kahdennettuja komponentteja ovat pääosin sellaiset, joissa on liikkuvia osia ja ovat siten alttiina mekaaniselle kulumiselle ja rikkoutumiselle. Tällaisia komponentteja ovat kiintolevyt, virtalähteet ja tuulettimet. Kahdennuksen ansiosta komponentin hajotessa toinen vastaava pitää järjestelmän edelleen toimintakuntoisena. Usein kahdennetut komponentit ovat vaihdettavissa ilman, että laitteistoa tarvitsee sammuttaa tai sen toimintaan muuten puuttua.

Palvelimien suorittimet, muistit, kiintolevyt ym. komponentit ovat usein nopeampia kuin työasemissa ja niiden määrä on suurempi. Yksi lisäkomponenttien haittapuolista on

kuitenkin lisääntynyt lämpö. Hallitsematon lämpötilan nousu laitteistossa voi tuhota komponentteja hyvin nopeasti. Tästä syystä palvelimien jäähdytysjärjestelmät yleensä koostuvat useista redundanttisista tuulettimista, joiden pyörimisnopeutta voidaan säädellä tarpeen mukaan. Vähänkään isompien palvelinlaitteistojen kohdalla lämmöntuottoon on lähes poikkeuksetta varauduttu myös sijoittamalla laitteisto niille erikseen varattuun, ilmastoituun tilaan.

Isoissa palvelintoteutuksissa on myös yleistä, että kokonaisia palvelimia on kahdennettu. Jos tällöin yksi palvelin syystä tai toisesta vikaantuu, voi toinen vastaava palvelin ottaa sen paikan lähes välittömästi. Tällöin on myös yleistä, että palvelimet suorittavat kuormanjakoa, jolloin kuormitus jakautuu tasaisesti palvelimien kesken. [6, s. 216-217, 260.]

4 Käyttöjärjestelmä Windows Server 2008

4.1 Yleistä

Windows Server on nykyinen tuotenimi Microsoftin palvelinkäyttöjärjestelmille. Nimeä käytettiin ensimmäisen kerran vuonna 2003 julkaistussa Windows Server 2003 –käyttöjärjestelmässä. Sen seuraaja on nykyinen, vuonna 2008 julkaisu Windows Server 2008, joka pohjautuu samaan Windows NT (New Technology) 6.0 –rakenteeseen kuin PC-käyttöjärjestelmä (Personal Computer) Windows Vista.

Vuonna 2009 julkaistiin päivitetty versio nimeltä Windows Server 2008 R2, joka on tällä hetkellä Microsoftin uusin palvelinkäyttöjärjestelmä. Tällä hetkellä Microsoftin uusimman PC-käyttöjärjestelmän Windows 7:n tavoin R2-versio pohjautuu Windows NT 6.1 -rakenteeseen. Windows Server 2008 R2 on saatavilla vain 64-bittisenä. Aikaisempien versioiden tapaan palvelinkäyttöjärjestelmästä on saatavilla useita versioita erilaisiin käyttötarkoituksiin. Eri versioista löytyy lisätietoa Microsoftin internetsivuilta.

Tämän insinöörityön palvelintoteutukseen on valittu Windows Server 2008 R2 -käyttöjärjestelmä, mistä johtuen tämän raportin sisältö koskee juuri kyseistä käyttöjärjestelmää, ellei toisin mainita. Puhuttaessa pelkästä käyttöjärjestelmästä

tarkoitetaan tässä raportissa juuri Windows Server 2008 R2 -käyttöjärjestelmää. Käyttöjärjestelmän ominaisuuksista on usein mainittu suluissa niiden englanninkielinen nimi, koska käyttöjärjestelmää ei ole saatavilla suomenkielisenä. Käyttöjärjestelmän valintaperusteet esitellään luvussa 6.2. [11, s. 44; 12.]

4.2 Levytyypit ja ja tiedostojärjestelmät

Levytyypit

Käyttöjärjestelmä tukee kahta eri levytyyppiä: peruslevyt ja dynaamiset levyt. Kiintolevyn levytyyppiä voidaan muuttaa esimerkiksi käyttöjärjestelmän levynhallintakonsolista. Peruslevy voidaan milloin tahansa muuttaa dynaamiseksi ilman, että sen sisältö tuhoutuu. Dynaamisen levyn muuttaminen peruslevyksi aiheuttaa aina sisällön tuhoutumisen. Levyn varmuuskopiointi on suositeltavaa aina levytyyppiä muutettaessa. Samassa tietokoneessa voi olla molempia levytyyppejä, mutta jos levyjä käytetään yhdessä esimerkiksi RAID-toteutuksessa, on käytettävien levyjen oltava samaa tyyppiä.

Peruslevy on perinteinen levytyyppi, jossa levy voidaan jakaa osioihin. Osio on kiintolevyn osa, joka toimii erillisenä tallennusyksikkönä, esimerkiksi loogisena levyasemana. Peruslevylle voidaan luoda ensisijaisia ja jatkettuja osioita. Ensisijaisia osioita voidaan käyttää tiedon tallennukseen luomalla niihin tiedostojärjestelmä alustuksen yhteydessä. Jatkettuja osioita ei voi sellaisenaan käyttää tiedon tallentamiseen, vaan niille luodaan yksi tai useampi looginen asema, joihin tiedostot tallennetaan.

Dynaamiset levyt tarjoavat peruslevyihin verrattuna lisäominaisuuksia levyjen käsittelyyn, kuten niiden peilauksen, lomituksen ja lomituksen pariteetilla. Dynaamisen levyn kokoa on voi myös muuttaa ilman, että tietokonetta tarvitsee käynnistää uudelleen. Nämä ominaisuudet ovat käytettävissä käyttöjärjestelmän levynhallintakonsolista. [11, s. 685-689.]

Osiointitavat

Windows-käyttöjärjestelmien kiintolevyissä käytetään kahta osiointitapaa: Master Boot Record (MBR) ja GUID Partition Table (GPT). Osiointitavat määrittelevät, miten osioinnin tiedot tallennetaan. Kun uusi, käyttämätön kiintolevy tuodaan järjestelmään, täytyy se alustaa ja valita sille osiointitapa. Osiointitavan voi vaihtaa esimerkiksi käyttöjärjestelmän levynhallintakonsolista. Sillä, onko kiintolevy dynaaminen vai peruslevy, ei ole merkitystä.

Master Boot Record (MBR) on vanha, x86- ja x64-pohjaisten tietokoneiden käyttämä ja kaikkien Microsoftin työasema- ja palvelinkäyttöjärjestelmien tukema osiointitapa. MBR tukee enimmillään 2 tebitavun suuruisia osioita. Levyllä voi olla enimmillään neljä ensisijaista osiota, tai kolme ensisijaista ja yksi jatkettu osio.

GUID Partition Table (GPT) on uudempi osiointitapa, jolle löytyy tuki Windows Server 2003 SP1 ja Windows Vista -käyttöjärjestelmistä lähtien. GPT toimii MBR:n tapaan sekä x86- että x64-pohjaisissa järjestelmissä. GPT tukee enimmillään 18 eksbitavun suuruisia osioita, joita voi olla Windows-käyttöjärjestelmässä 128 kappaletta. GPT:n osiointitaulukon kahdennus ja CRC-suojaus tarjoaa parempaa luotettavuutta, kuin MBR. [6, 219-221; 11, s. 690-691.]

Tiedostojärjestelmät

Tiedostojärjestelmä on käyttöjärjestelmän ylläpitämä palvelu, jonka avulla muut ohjelmistot voivat tallentaa tietoa kiintolevyille tai muille massamuisteille. Tiedostojärjestelmä peittää massamuistilaitteen teknisen rakenteen ja näyttää sen sisällön tiedostoina ja kansioina. Windows Server 2008 –käyttöjärjestelmä tukee CDFS-, UDF-, NTFS-, FAT-, FAT32-, FATX- ja exFAT-tiedostojärjestelmiä.

CDFS (Compact Disk File System) on ISO (International Organization for Standardization) 9660 -standardiin viittaava tiedostojärjestelmä, joka on nimensä mukaisesti käytössä CD-levyissä (Compact Disk). Myös DVD-levyt (Digital Versatile Disc) voivat käyttää käyttää CDFS-tiedostojärjestelmää, mutta sellaisen levyn alustaminen ei ole tuettu toimenpide Windows Server 2008 -käyttöjärjestelmässä.

UDF (Universal Disk Format) on ISO/IEC (International Electrotechnical Commission) 13346 -standardin toteutus, jota käytetään uudelleenkirjoitettaville optisille medioille, kuten DVD-levyille eri variaatioineen. Käyttöjärjestelmän levynhallintakonsoli mahdollistaa levyjen alustamisen UDF-tiedostojärjestelmän eri versioilla.

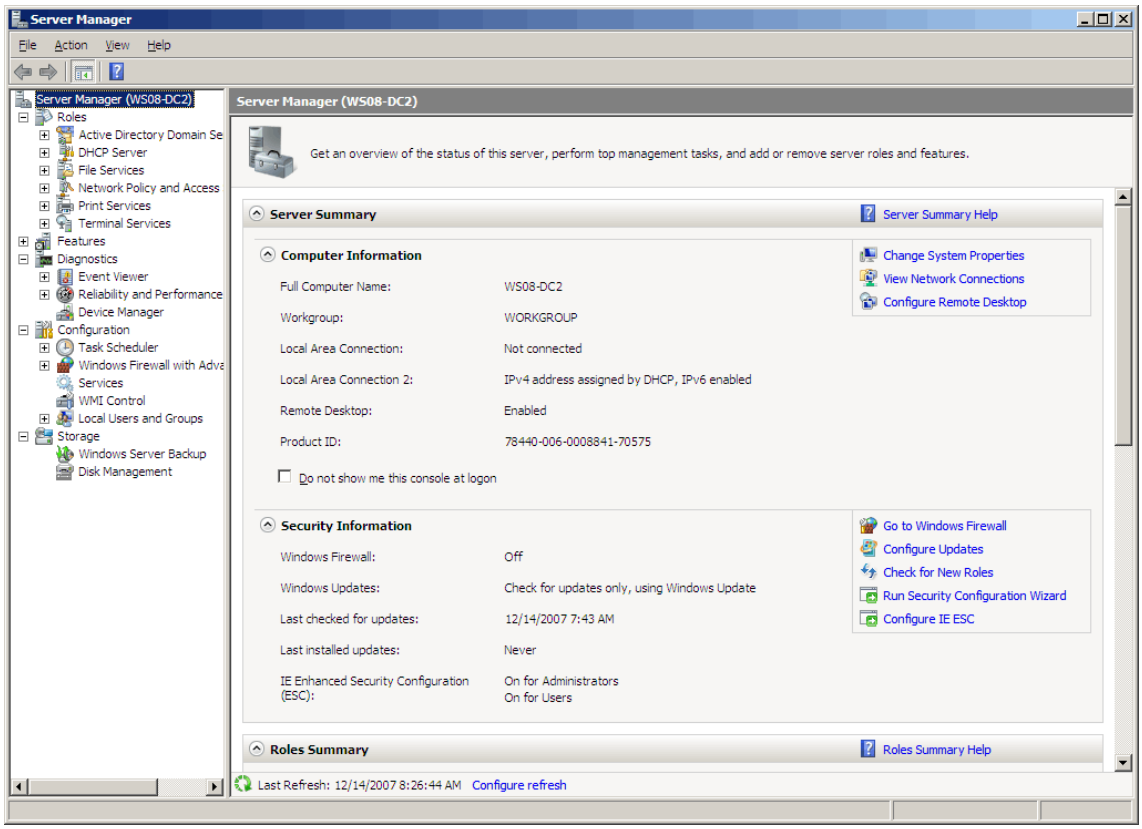
NTFS (New Technology File System) on Microsoftin kehittämä ja Windows-käyttöjärjestelmien oletusarvoinen tiedostojärjestelmä Windows 2000 -versiosta lähtien. NTFS tarjoaa tiedosto- ja kansiokohtaisia suojauksia, levyn pakkaamista, levykiintiöitä ja salausta.

FAT (File Allocation Table) on Microsoftin vuonna 1977 kehittämän tiedostojärjestelmä, joka edelsi NTFS:ää Windows-käyttöjärjestelmien oletusarvoisena tiedostojärjestelmänä. FATista on useita erilaisia versioita, kuten Xbox-pelikonsolissa käytetty FATX ja muistitikuille tarkoitettu exFAT. Myös FAT32 on nykyään käytössä lähinnä muistitikuissa. [11, s. 722-727.]

4.3 Käyttöjärjestelmän hallinta

Hallintakonsoli

Hallintakonsoli (Server Manager) on Windows Server 2008 -käyttöjärjestelmän keskitetty työkalu palvelimen hallintaan. Hallintakonsoli näyttää esimerkiksi palvelimen laitteiston, asetukset, asennetut roolit ja ominaisuudet sekä näihin liittyvät keskeiset tapahtumat. Hallintakonsolista voidaan asentaa, muokata ja poistaa palvelimen rooleja, roolipalveluita ja ominaisuuksia. Hallintakonsolilla on myös sitä vastaava komentorivityökalu ServerManagerCmd.exe. Graafisen hallintakonsolin yhteenvetoikkuna näkyy kuvassa 5.



Kuva 5. Hallintakonsolin yhteenvetonäkymä [13].

Hallintakonsoli käynnistyy oletuksena automaattisesti, kun järjestelmänvalvoja kirjautuu sisään. Poikkeuksena on heti käyttöjärjestelmän asennuksen jälkeinen käynnistys, jolloin automaattisesti käynnistyy karsitumpi Initial Configuration Tasks -työkalu. Initial Configuration Tasks -työkalun ikkunassa on valintaruutu sille, halutaanko sen käynnistyvän myös jatkossa. Myös hallintakonsolin automaattinen käynnistyminen voidaan ottaa pois päältä samalla tavalla.

Windows Server 2008 –versiossa hallintakonsoli mahdollistaa vain paikallisen palvelimen hallinnan, joten haluttaessa hallita toista palvelinta on käytettävä etätyöpöytää tai erillisiä hallintakonsoleita. Windows Server 2008 –käyttöjärjestelmän uudemmassa R2-versiossa hallintakonsolilla voidaan hallita myös muita palvelimia, kunhan etähallinta on sallittu. Etäyhteyksien toimintaa esitellään luvussa 5.3.

Roolit, roolipalvelut ja ominaisuudet

Palvelinroolit (Server roles) ovat käyttöjärjestelmään asennettavia ohjelmistokomponentteja, jotka mahdollistavat erilaisia palvelintoiminnallisuuksia ja siten muodostavat ison osan palvelimen toiminnasta. Tällaisia toiminnallisuuksia ovat esimerkiksi DHPC-, tietokanta- ja web-palvelin. Oletuksena käyttöjärjestelmään ei ole asennettu mitään rooleja, mutta ilman roolejakin on mahdollista jakaa levyasemia ja tulostimia, eli toimia tiedosto- ja tulostinpalvelimena. Palvelimella voi olla useampia rooleja samanaikaisesti.

Roolipalvelut (Role services) ovat rooleja pienempiä ohjelmistokomponentteja, jotka tarjoavat toiminnallisuuksia palvelinrooleille. Tietyillä rooleilla, kuten DHCP:llä on vain yksi roolipalvelu eli toiminnallisuus, jolloin roolin asentaminen sisältää tarvittavan roolipalvelun asennuksen. Toiset roolit taas sisältävät ja mahdollisesti edellyttävät useampia roolipalveluita. Esimerkiksi tulostuspalvelut-rooliin voidaan asentaa Internet Printing –roolipalvelu, joka mahdollistaa verkkopohjaisten tulostustoimintojen käytön.

Ominaisuudet (Features) ovat valinnaisesti asennettavia, rooleja pienempiä komponentteja. Ominaisuudet ovat usein yksittäisiä työkaluja tai tapoja tuoda jokin palvelu esille ja käytettäväksi. Ominaisuuksia ovat esimerkiksi BitLocker ja SMTP-palvelin (Simple Mail Transfer Protocol). BitLocker on salaustyökalu, jonka toimintaa esitellään luvussa 4.4.2. SMTP-palvelin-ominaisuudella palvelin voi välittää ja reitittää sähköpostiviestejä. Roolipalvelujen tapaan jotkin roolit edellyttävät tiettyjä ominaisuuksia toimiakseen.

Rooleja, roolipalveluita ja ominaisuuksia voi asentaa hallintakonsolin lisäksi ensimmäisen käynnistyksen yhteydessä avautuvalla Initial Configuration Tasks -työkalulla sekä hallintakonsolin komentoriviversiolla. Muokkaaminen ja poistaminen on mahdollista vain hallintakonsolilla. [11, s. 409-443.]

4.4 Tietoturva

4.4.1 Virustorjunta ja palomuuri

Palvelinkäyttöjärjestelmien ohjelmallinen virustorjunta koostuu työasematietokoneiden tapaan virustorjuntaohjelmistosta, palomuurista ja mahdollisesti haittaohjelmien

torjuntaohjelmistosta. Virustorjuntaohjelmistot suojaavat myös muilta vakavilta haittaohjelmatyypeiltä kuin viruksilta, mutta virustorjunnasta on muodostunut kyseisten ohjelmistojen yleisnimitys. Palomuuri pitää vain tarvittavat verkkoliikenteen portit avoinna ja valvoo tietokoneen verkkoliikennettä tietomurtojen ja muiden haitallisten tapahtumien varalta.

Erilliset haittaohjelmien torjuntatyökalut on tarkoitettu lähinnä vakoilu- ja mainosohjelmien torjuntaan, eivätkä siten suojaa esimerkiksi viruksilta. Haittaohjelmien torjuntatyökalu voi kuitenkin olla tarpeellinen lisä virustorjunnalle, koska ne ovat useasti tehokkaampia löytämään vähemmän haitallisia ohjelmia, kuten mainosohjelmia. Tällaiset haittaohjelmat tarttuvat yleensä internet-sivuilta, joten torjuntaohjelmiston tarpeellisuus riippuu paljon palvelimen käytöstä.

Windows Server 2008 -käyttöjärjestelmä sisältää valmiiksi palomuurin ja vakoiluohjelmien torjuntaan tarkoitetun Windows Defenderin, mutta ei virustorjuntaohjelmistoa. Microsoft tarjoaa kuitenkin ilmaisen Security Essentials -virustorjuntaohjelmiston pienyrityksille, joilla on käytössä enintään 10 suojattavaa tietokonetta.

Palvelimen virustorjunnaksi soveltuu käytöstä riippuen joko normaali työasemien virustorjuntaohjelmisto, tai erityisesti palvelimille suunniteltu versio. Palvelimille tarkoitettu virustorjuntaohjelmisto voi olla suunniteltu esimerkiksi tiedostopalvelimen toimintaa varten. Palvelimien virustorjuntaratkaisuja tarjoavat useat tunnetut virustorjuntaohjelmistojen valmistajat. [11, s. 107.]

4.4.2 Salaus

Palomuurin avulla voidaan määrittää, mitkä verkkoliikenteen portit pidetään avoinna ja mitkä suljettuina. Kuitenkin verkkoyhteyden ja sovellusten toiminta edellyttää tiettyjen porttien jättämistä avoimiksi, mikä on otettava huomioon tietoturvaa suunniteltaessa. Tiedon salausmenetelmät mahdollistavat tietojen suojaamisen vielä siinä tilanteessa, jossa ulkopuolinen on päässyt järjestelmän sisälle. Useimmiten salaamisen tarkoituksena on saada tieto muotoon, josta vain tiedon vastaanottaja saa palautettua alkuperäisen tiedon.

Windows Server 2008 -käyttöjärjestelmä sisältää kaksi hieman erilaista salaustyökalua, joista ensimmäinen ja vanhempi on salaava tiedostojärjestelmä EFS (Encrypting File System). EFS:n avulla käyttäjä voi salata haluamansa kansiot ja tiedostot niin, ettei kukaan muu pysty niitä käyttämään.

BitLocker

Toisin kuin EFS, uudempi BitLocker ei ole tarkoitettu kansioiden ja tiedostojen suojaamiseksi tietylle käyttäjälle niin, etteivät muut pysty niitä käyttämään. BitLockerin tarkoitus on suojata kokonaisia asemia tai koko järjestelmää ulkopuolisilta henkilöiltä, esimerkiksi varkauden varalta. Jos esimerkiksi kiintolevy varastetaan ja asennetaan toiseen tietokoneeseen, BitLocker lukitsee suojatut tiedot estäen kaiken pääsyn niihin. Jos taas kiintolevyä käytetään BitLockerin tunnistamassa tietokoneessa, niin kaikilla on pääsy kiintolevyn tietoihin, joten käyttöoikeuksien ja EFS:n käyttö on tarpeellista.

BitLockerin käyttö vaatii kiintolevyltä erillisen, vähintään 1,5 GiB suuruisen järjestelmäosion, johon se tallentaa käynnistyksen vaatimia tiedostoja. Lisäksi kaksi BitLockerin toimintatavoista vaatii tietokoneelta TPM-piirin (Transfer Platform Module) 1.2 tai uudemman version ja sen kanssa yhteensopivan BIOSin (Basic Input Output System). TPM-piiri on erillinen suoritin tai mikropiiri, joka säilyttää salausavaimia. BIOS on tietokoneohjelma, joka aloittaa koodin suorittamisen, kun tietokone käynnistetään.

BitLockerilla on seuraavat kolme toimintatapaa:

- Läpinäkyvä (transparent): Järjestelmä tallentaa BitLockerin salausavaimen TPM-piirille ja käyttää sitä automaattisesti, kun käynnistysympäristö on todettu muuttumattomaksi. Tämä sallii järjestelmän käynnistyksen eikä käyttäjältä vaadita mitään toimia.
- Käyttäjän tunnistus (user authentication): Salausavain tallennetaan TPM-piirille, mutta käyttäjän on syötettävä PIN-koodi (Personal Identification Number) tai valtuutettu USB-avain järjestelmän käynnistämiseksi.
- USB-avain (USB key): Järjestelmä tallentaa käynnistysavaimen USB-muistille, joka käyttäjän on syötettävä järjestelmän käynnistämiseksi. Tämä tapa ei vaadi

TPM-piiriä, mutta tietokoneen BIOSin on tuettava USB-muistin käyttöä käynnistyksessä.

Microsoftin mukaan BitLockerin salaus ei sisällä ns. takaovea, joka mahdollistaisi salauksen purkamisen kolmansille osapuolille, kuten lainvalvojille. Microsoft ei ole kuitenkaan julkistanut sen lähdekoodia, joten tietoa ei ole voitu varmistaa itsenäisten tutkijoiden toimesta. [6, s. 301-303.]

4.4.3 Tunnistus ja valtuutus

Tunnistus

Käyttäjän tunnistaminen on oleellinen osa toimivaa ja tietoturvallista järjestelmää. Tunnistetiedot säilytetään toteutuksesta riippuen joko suoraan sillä palvelimella, johon käyttäjät kirjautuvat, tai keskitetysti verkossa esimerkiksi aktiivihakemistopalvelimen toimesta. Kaikissa toteutuksissa tunnistetiedot säilytetään palvelimella salattuina, jolloin tietomurrossa onnistuessaan hyökkääjä joutuu vielä purkamaan salaukset päästäkseen käsiksi tunnistetietoihin.

Jotta käyttäjä voidaan tunnistaa, on hänen ilmoitettava ja todistettava henkilöllisyytensä. Henkilöllisyys ilmoitetaan yleensä käyttäjätunnuksella tai sähköpostilla ja todistetaan joko salasanalla, älykortilla tai biometrisella tunnisteella. Älykortti on luottokortin kokoinen laite, jonka muistipiirit mahdollistavat esimerkiksi salausavaimen tallentamisen. Biometrinen tunniste on yleensä joko sormenjälki, silmän verkkokalvo tai käyttäjän kasvot.

Salasanat voidaan kuitenkin arvata ja älykortit varastaa, joten yksi tunnistusmenetelmä ei välttämättä ole riittävä. Useamman menetelmän käyttäminen vähentää huomattavasti sitä mahdollisuutta, että ulkopuolinen henkilö pystyisi tunnistautumaan toisen henkilön tiedoilla. Yleisin menetelmien yhdistelmä on älykortin ja salasanan käyttö yhdessä. Useamman menetelmän yhdistelmä on suositeltavaa ainakin järjestelmänvalvojille, koska heidän käyttöoikeutensa ovat huomattavasti normaalia käyttäjää laajemmat.

Älykorttien käyttö voi kuitenkin aiheuttaa ongelmia joidenkin sovellusten kanssa. Jos sovellukselle on myönnetty Certified for Windows Server 2008 -logo, se on testattu yhteensopivaksi käyttöjärjestelmän turvastandardien ja älykorttien kanssa.

Jotta voidaan varmistua käyttäjien salasanojen turvallisuudesta, on järjestelmänvalvojilla mahdollisuus asettaa salasanoille tiettyjä vaatimuksia. Salasanavaatimuksien määrittämiseen käyttöjärjestelmä tarjoaa seuraavat vaihtoehdot:

- Uudelleenkäytön estäminen: Järjestelmä tallentaa käyttäjien salasanat ja estää heitä käyttämästä samoja salasanoja uudestaan. Oletusarvona järjestelmä tallentaa jokaisen käyttäjän 24 viimeisintä salasanaa.
- Enimmäisaika: Määrää kuinka kauan salasana voi olla käytössä, ennen kuin se on vaihdettava. Oletusarvo on 42 päivää.
- Vähimmäisaika: Määrää kuinka kauan salasanan on oltava käytössä, ennen kuin se voidaan vaihtaa. Oletusarvo on 1 päivä.
- Vähimmäispituus: Määrää kuinka monta merkkiä salasanassa on vähintään oltava. Oletusarvo on 7 merkkiä.
- Monimutkaisuus: Pakottaa käyttäjän valitsemaan salasanan, joka ei ole käyttäjätunnus tai osa siitä, on vähintään 6:en merkin pituinen ja sisältää merkkejä kolmesta seuraavasta kategoriasta: isot kirjaimet, pienet kirjaimet, numerot (0-9) ja erikoismerkit (esim. !, $, #, %). Monimutkaisuuden vaatimus on oletuksena käytössä.
- Palautettava salaus: Tallentaa salasanat sellaisella salauksella, joka on helppo purkaa salasanatietoja tarvitsevien sovellusten toimesta. Tämä aiheuttaa huomattavan tietoturvariskin ja sitä tulisi käyttää vain, jos se on varmasti tarpeellinen. Tämä ominaisuus on oletuksena poissa käytöstä.

Salasanojen vaatimuksia suunnitellessa on syytä ottaa huomioon käyttäjien kyky muistaa salasanansa. Pitkä ja monimutkainen salasana, joka vaihtuu usein, on käyttäjälle vaikea muistaa ja siten todennäköisempi päätymään esimerkiksi muistilapulle. [6, s. 305-311.]

Valtuutus

Valtuutus tarkoittaa sen selvittämistä, onko tunnistautuneella käyttäjällä oikeus suorittaa haluttu toimenpide. Toimenpide voi olla esimerkiksi tiedoston avaaminen tai tulostaminen, ja jokaisen toimenpiteen kohdalla käyttöjärjestelmä tarkistaa, onko käyttäjällä oikeus sen suorittamiseen. Valtuutus on ymmärrettävästi iso osa tietoturvaa ja käyttöjärjestelmän konfigurointia, koska käyttäjien tarpeet ja heille halutut oikeudet ovat hyvin erilaisia.

Windows Server 2008 sisältää valtuuttamiseen useita eri tyyppisiä oikeuksia. Oikeustyypit ovat seuraavat:

- Jako: Hallitsee tiedostoihin ja kansioihin pääsyä verkon kautta.
- NTFS: Hallitsee tiedostoihin ja kansioihin pääsyä levyasemilla, jotka ovat alustettu NTFS-tiedostojärjestelmällä.
- Rekisteri: Hallitsee pääsyä tiettyihin osiin käyttöjärjestelmän rekisterissä. Näitä tarvitsee esimerkiksi sovellus, joka tekee muutoksia käyttöjärjestelmän rekisteriin.
- Aktiivihakemisto: Hallitsee pääsyä tiettyihin osiin aktiivihakemistossa.

Kaikki oikeustyypit toimivat toisistaan riippumatta ja välillä yhdessä suojatakseen tiettyä resurssia. Jos esimerkiksi käyttäjälle annetaan NTFS-oikeudet palvelimella sijaitsevaan tiedostoon, pystyy hän käyttämään sitä kirjautumalla omilla tunnuksillaan kyseiselle palvelimelle. Jos käyttäjä kuitenkin yrittää päästä tiedostoon käsiksi omalta, palvelimen verkkoon liitetyltä tietokoneeltaan, vaatii tiedostoon pääsy vielä lisäksi jako-oikeudet. Tiedoston käyttäminen verkon yli vaatii siis aina sekä NTFS- että jako-oikeudet.

Määritetyt oikeudet tallennetaan kunkin resurssin pääsylistaan (Access Control List, ACL). Jokainen tallennettu oikeus (Access Control Entry, ACE) sisältää valitun käyttäjän, ryhmän tai tietokoneen ja tarkkaan määritetyt oikeudet sekä rajoitukset. Resurssien oikeudet ovat periytyviä, jolloin esimerkiksi tietylle kansiolle määritetty lukuoikeus koskee myös sen alikansioita ja tiedostoja.

Resurssien oikeuksia määritetään niiden ominaisuuksista löytyvän turvallisuus-välilehden (security) avulla. Eri käyttäjille, ryhmille tai tietokoneille voidaan määrittää esimerkiksi pelkkä lukuoikeus, oikeus muokata, oikeus suorittaa tai ei oikeuksia

ollenkaan, jolloin resurssi ei ole edes näkyvissä. Käyttäjäryhmien luominen ja niille oikeuksien määrittäminen on usein kannattavampaa, kuin oikeuksien määrittäminen erikseen jokaiselle käyttäjälle. [6, s. 317-322.]

4.4.4 Varmuuskopiointi

Varmuuskopioinnin tarkoitus

Varmuuskopiointi on oleellinen osa järjestelmän ylläpitoa ja suojausta, koska tietojen menettäminen tai työläs palauttaminen voi aiheuttaa esimerkiksi yritykselle taloudellisen menetyksen. Varmuuskopioinnilla varmistetaan tiedonsaanti, jos syystä tai toisesta alkuperäinen tallenne tuhoutuu.

Tiedot voivat tuhoutua monesta syystä. Tietokoneen käyttäjä voi vahingossa poistaa tai korvata vääriä tiedostoja. Tietokoneen kiintolevy, DVD-levy tai muu tallennusväline voi rikkoutua tai siihen voi tulla toimintavika, jolloin sille talletettuja tiedostoja ei enää voi käyttää. Ikuista tallennusvälinettä ei ole keksitty ja tuskin keksitäänkään. Tietokone voi myös rikkoutua fyysisesti esimerkiksi tulipalossa. Tiedostoja ja laitteita voi myös kadota ja niitä voidaan varastaa. Myös virukset ja muut haittaohjelmat voivat aiheuttaa tiedostojen katoamisen.

Varmuuskopiointi täytyy suorittaa riittävän usein. Ihanteellisesti aina, kun tieto muuttuu. Näin tiedostoista on aina tuorein versio tallessa ja mahdollisimman vähän työtä menee hukkaan, jos vahinko sattuu. Varmuuskopioita tulee säilyttää eri paikassa kuin alkuperäistä tietoa, jolloin esimerkiksi tulipalo ei samanaikaisesti tuhoa molempia.

Säännöllisen varmuuskopioimisen lisäksi on syytä opetella ja kokeilla tietojen palauttamista varmuuskopiosta. Mikään ei tarjoa varmempaa tietoa varmuuskopioiden toimivuudesta kuin testipalautukset. Näin myös säästetään aikaa vahingon sattuessa, koska palauttamisen vaatimat toimenpiteet ovat hyvin hallussa.

Varmuuskopiointimenetelmät

Varmuuskopioinnin tekemiseen on laitteistosta riippumatta useampia menetelmiä, jotka sopivat erilaisiin tilanteisiin. Menetelmien vaatimaan aikaan ja tallennusresursseihin pätee käytännössä seuraava sääntö: mitä enemmän aikaa ja resursseja varmistaminen vaatii, sitä nopeampaa on tiedon palauttaminen.

Täysi varmistus on menetelmä, jolla varmistetaan koko tiedostojärjestelmä tai jokin kokonainen osio siitä. Täysi varmistus on tyypillisesti järjestelmän ylläpidon perustoimi. Täyden varmistuksen etuna on se, että kaikki tiedostot ja kansiot varmistuvat kerralla, jolloin palauttaminen on yksinkertaista. Haittapuolena voidaan pitää sitä, että tallentaminen vaatii muita menetelmiä enemmän aikaa ja laitteistoresursseja.

Inkrementaalinen varmistus tarkoittaa menetelmää, jolla kopioidaan ainoastaan ne tiedostot ja kansiot, jotka ovat muuttuneet tai jotka on luotu edellisen varmuuskopioinnin jälkeen. Edeltävän varmuuskopion tekemiseen käytetty menetelmä ei vaikuta inkrementaalisen varmistuksen toimintaan. Inkrementaalinen menetelmä vaatii tallentaessa vähemmän aikaa ja resursseja kuin täysi varmistus, mutta tietojen palauttaminen on hitaampaa. Haittapuolena on myös se, että varmuuskopioinnista ei jää yhtenäistä näkymää, koska vain osa tiedoista varmistetaan.

Differentiaalinen varmistus on menetelmä, jolla varmuuskopioidaan kaikki täyden varmistuksen jälkeen muutetut tai luodut tiedot. Varmistusprosessi vaatii enemmän resursseja kuin inkrementaalinen varmistus, mutta kuitenkin vähemmän kuin täysi varmistus. Myös differentiaalisen menetelmän huonona puolena on palauttamisen monimutkaisuus, koska varmuuskopio ei sisällä kaikkia tietoja.

Varmuuskopiointiohjelmisto

Windows Server 2008 -käyttöjärjestelmä sisältää Windows Server Backup Features -ominaisuuden, johon kuuluu varmuuskopiointiohjelma Windows Server Backup. Varmuuskopiointiohjelma asennetaan palvelimen hallintakonsolista ja siitä on valittavissa graafinen versio ja komentoriviversio.

Varmuuskopiointiohjelma on suunniteltu lähinnä koko järjestelmän varmuuskopioimiseksi erilliselle kiintolevylle, mistä johtuen siinä on seuraavia huomion arvoisia asioita:

- Ajastetun varmuuskopioinnin kohteena ei voi olla optinen media, kuten DVD-asema. Nauha-asemia ei tueta ollenkaan.
- Vain koko asemia voidaan varmuuskopioida, eli yksittäisiä kansioita ja tiedostoja ei voi valita. Varmuuskopioista voidaan kuitenkin palauttaa yksittäisiä kansioita ja tiedostoja.
- Tuetut varmuuskopiointimenetelmät ovat ainoastaan täysi ja inkrementaalinen. Kaikille varmuuskopiointitehtäville täytyy määrittää sama varmuuskopiointimenetelmä. Eri asemille voi kuitenkin määrittää eri varmuuskopiointimenelmät.
- Vain yksi varmuuskopiointitehtävä voidaan ajastaa ja se voidaan suorittaa joko päivittäin tai useamman kerran päivässä. Varmuuskopiointitehtävää ei voi ajastaa tulevalle päivämäärälle, eikä tehtävien välistä aikaa voi määrittää 24:ää tuntia suuremmaksi.
- Varmuuskopiot tallennetaan VHD-muodossa (Virtual Hard Disk) ja ainoastaan sen mukaisia varmuuskopioita voidaan palauttaa. Tästä johtuen esimerkiksi Windows Server 2003 -käyttöjärjestelmän varmuuskopiointiohjelmalla tallennettuja varmuuskopioita ei voida palauttaa.
- Varmuuskopioinnin kohteeksi valittu kiintolevy alustetaan ja rajoitetaan vain varmuuskopiointiohjelman käyttöön, jolloin kiintolevyn aikaisemmat tiedot poistetaan eikä sitä voi käyttää muuhun tarkoitukseen.

Monipuolisempaa varmuuskopiointia varten Microsoft tarjoaa System Center Data Protection Manager -ohjelmistoa. Markkinoilla on myös paljon muiden valmistajien ohjelmistoja, jotka mahdollistavat joustavamman varmuuskopioimisen. [6, s. 470-472; 11, s. 1151-1152.]

Varjokopiot

Varmuuskopiot ovat ensisijaisesti suojautumiskeino isojen menetyksien kuten laitteiston rikkoutumisen tai varkauden varalle. Kuitenkin yksittäisten tiedostojen menettäminen on kaikkein yleisintä, johtuen tyypillisesti käyttäjien virheistä.

Varmuuskopioista vastaavalle henkilöstölle yksittäisten tiedostojen palauttaminen voi olla säännöllinen vaiva ja toteutuksesta riippuen jopa varsin työläs sellainen.

Tämän ongelman ratkaisemiseksi käyttöjärjestelmä sisältää ominaisuuden nimeltä varjokopio (Shadow Copy). Varjokopio säilyttää tiedostoista useita aikaisempia versioita tietyiltä ajankohdilta, minkä ansiosta kadonneet tai muuttuneet tiedostot pystytään usein palauttamaan. Tiedoston aikaisemmat versiot näkyvät myös käyttäjälle, joka voi itsekin suorittaa palautuksen varjokopion avulla. Varjokopioita hyödynnetään myös normaalissa varmuuskopioimisessa silloin, kun varmuuskopioitava tiedosto on lukittu toisen sovelluksen käyttöön.

Oletuksena varjokopio ei ole käytössä millään tiedostoilla ja se voidaan määrittää ainoastaan koko asemille yksittäisten tiedostojen sijaan. Oletuksena varjokopio varaa valitulta asemalta 10 % tallennustilaa tiedostoja varten ja ottaa niistä kopiot joka arkipäivä kello 7:00 ja 24:00. Tallennustilan suuruuden ja tiedostojen kopiointiajankohdan lisäksi myös kopioiden tallennuskohde voidaan määrittää itse.

Työasematietokoneissa tarvitaan lisäksi varjokopioasiakasohjelma, joka on sisäänrakennettu ominaisuus Windows Vistassa ja sitä uudemmissa Windows-käyttöjärjestelmissä. Vanhemmille käyttöjärjestelmille asiakasohjelma on saatavilla Microsoftin internet-sivuilta. [6, s. 252; 11, s. 818-819.]

5 Käyttömahdollisuudet

5.1 Aktiivihakemisto

Toiminta

Aktiivihakemisto (Active Directory) on Microsoft Windows Server -käyttöjärjestelmissä käytetty hakemistopalvelu. Hakemistopalvelu on säilytyspaikka tiedoille verkkoon liitetyistä resursseista, joita ovat laitteisto, ohjelmisto ja käyttäjät. Nämä resurssit käyttävät hakemistopalvelua erilaisiin tarkoituksiin, kuten käyttäjien tunnistamiseen ja tiedon jakamiseen. Hakemistopalvelun toimintaympäristö voi olla esimerkiksi yrityksen verkko tai sen osa.

Aktiivihakemiston ensisijaisia tehtäviä on tuoda palvelut ja resurssit saataville, sekä tarjota tunnistus- ja valtuutuspalvelua verkon resursseille. Tämä tarkoittaa esimerkiksi käyttäjien tunnistamista ja käyttöoikeuksien valvomista.

Aktiivihakemistoon liitetyt käyttäjät kirjautuvat aktiivihakemiston alueeseen (Active Directory domain) yksittäisen tietokoneen tai sovelluksen sijaan. Käyttäjillä on pääsy kaikkiin niihin alueen resursseihin, joihin heille on myönnetty oikeudet. Ilman aktiivihakemistoa käyttäjillä pitäisi olla erilliset käyttäjätilit jokaisella käyttämällään tietokoneella, mikä olisi työlästä ja ongelmallista käyttäjätilien luomisen ja hallitsemisen kannalta.

Kun käyttäjä kirjautuu aktiivihakemiston alueeseen, käyttäjän tietokone suorittaa tarkan tunnistautumisprosessin, joka käsittää lähimmän alueen ohjauspalvelimen etsimisen ja sen kanssa kommunikoinnin käyttäen Kerberosta. Kerberos on monimutkainen tietoturvaprotokolla. Useimmiten käyttäjä tunnistautuu salasanalla, mutta aktiivihakemisto tukee myös tunnistautumista älykorteilla ja biometrisilla tunnisteilla.

Onnistuneen tunnistautumisprosessin jälkeen aktiivihakemisto suorittaa käyttäjän oikeuksien tarkistamisen aina, kun hän yrittää käyttää jotain verkon resurssia. Järjestelmänvalvoja myöntää käyttäjille oikeuksia resursseihin asettamalla heille käyttöoikeuksia. Käyttäjien ja suojattujen resurssien välillä ei tapahdu mitään ilman alueen ohjauspalvelimen toimintaa kolmantena osapuolena.

Arkkitehtuuri

Aktiivihakemisto on hierarkinen, alueisiin perustuva hakemistopalvelu, joka skaalautuu molempiin suuntiin. Aktiivihakemiston alue voidaan jakaa organisaatioyksikköihin (organizational units) ja ne voidaan täyttää objekteilla. Voidaan myös luoda useita alueita ja sisällyttää ne isompiin kokonaisuuksiin, joita ovat tontit (sites), puut (trees) ja metsät (forests). Skaalautuvuutensa ansiosta aktiivihakemisto tarjoaa hyvin joustavan arkkitehtuurin, joka sopii organisaatiolle sen koosta riippumatta.

Alueet (domains) ovat aktiivihakemiston perusta. Alue on looginen kokoelma niistä verkon resursseista, joita voidaan hallita ja jotka ovat samaa kokonaisuutta. Alue on hierarkinen, haarautuva rakenne, kuten esimerkiksi tiedostojärjestelmä. Alueella on aina vähintään yksi ohjauspalvelin (domain controller).

Objektit (objects) edustavat loogista tai fyysistä resurssia, joista alueiden ja muiden kokonaisuuksien sisältö koostuu. Objekteja on kahdenlaisia: haaraobjekteja (container objects) ja lehtiobjekteja (leaf objects). Haaraobjektien alaisuudessa voi olla muita objekteja, kun taas lehtiobjektilla ei. Kuvainnollisesti haaraobjektit muodostavat puun oksat ja lehdet kasvavat niistä.

Alueet ja organisaatioyksiköt itsessään ovat haaraobjekteja. Lehtiobjektit edustavat verkon resursseja, kuten käyttäjiä, tietokoneita ja ryhmiä.

Objektit koostuvat *attribuuteista (attributes)*, jotka sisältävät tietoa objektista. Haaraobjektin yksi attribuuteista sisältää listan kaikista sen alaisuudessa olevista objekteista. Lehtiobjektiivien attribuutit sisältävät tietoa niiden edustamasta resurssista, kuten käyttäjän nimi, osoite, puhelinnumero ja muut tunnistetiedot. [6, s. 92-93.]

5.2 DHCP-palvelin

DHCP (Dynamic Host Control Protocol) on lyhenne protokollasta, jolla verkkoon liitetyille laitteille jaetaan TCP/IP-asetuksia (Transmission Control Protocol / Internet Protocol).

DHCP-palvelimen jakamat TCP/IP-asetukset käsittävät vähintään asiakaslaitteen uniikin IP-osoitteen ja aliverkon peitteen, mutta yleensä myös oletusyhdyskäytävän ja nimipalvelimen tai nimipalvelimien IP-osoitteet. Asetukset voivat sisältää myös monia muita tietoja, kuten reitittimille käyttöjärjestelmän lataamiseen tarkoitetun palvelimen osoitteen.

DHCP:n toiminta koostuu seuraavasta kolmesta osasta:

1. DHCP-palvelin, joka pyynnöistä jakaa TCP/IP-asetuksia verkon laitteille.
2. DHCP-asiakas, joka pyytää TCP/IP-asetuksia palvelimelta ja ottaa ne käyttöön.

3. DHCP-protokolla, joka määrittää asiakkaan ja palvelimen välisen viestinnän muodon ja järjestyksen.

Puhuttaessa palvelimesta, asiakkaasta, protokollasta ja asetuksista tässä luvussa, tarkoitetaan niillä DHCP-palvelinta, DHCP-asiakasta, DHCP-protokollaa ja TCP/IP-asetuksia.

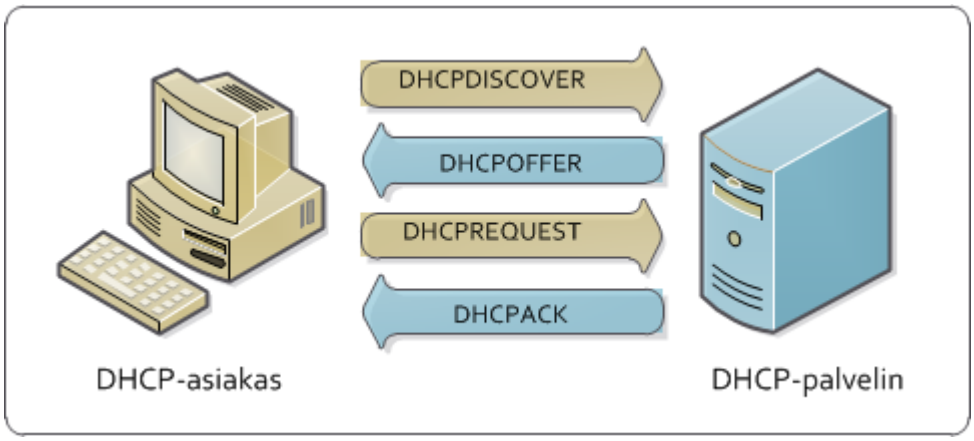
Palvelimelle määritetään osoitealueita, joista palvelin jakaa asiakaslaitteille IP-osoitteita. Yksittäinen palvelin voi hallita noin 1000 osoitealuetta ja palvella noin 10 000 asiakasta.

Useimmiten palvelimen jakamat osoitteet ovat lainoja, joilla on erääntymisajankohta. Laina-aika voidaan kuitenkin määritellä äärettömän pituiseksi. Toinen IP-osoitteiden jakamiseen käytetty tapa on varaus, jossa IP-osoite annetaan pysyvästi asiakkaalle siihen asti, kunnes varaus erikseen poistetaan.

Lainan erääntymisestä johtuen asiakas joutuu uusimaan lainansa säännöllisin väliajoin. Jos asiakas ei uusi lainaa, palvelin palauttaa IP-osoitteen jaettavien osoitealueeseen.

Asetusten jakaminen

Asiakkaan ja palvelimen välinen kommunikointi tapahtuu aina asiakkaan aloitteesta. Kuvassa 1 on havainnollistettu protokollan mukaisia viestejä asiakkaan ja palvelimen välillä. Asiakkaan pyytäessä asetuksia käsittää prosessi seuraavat vaiheet:

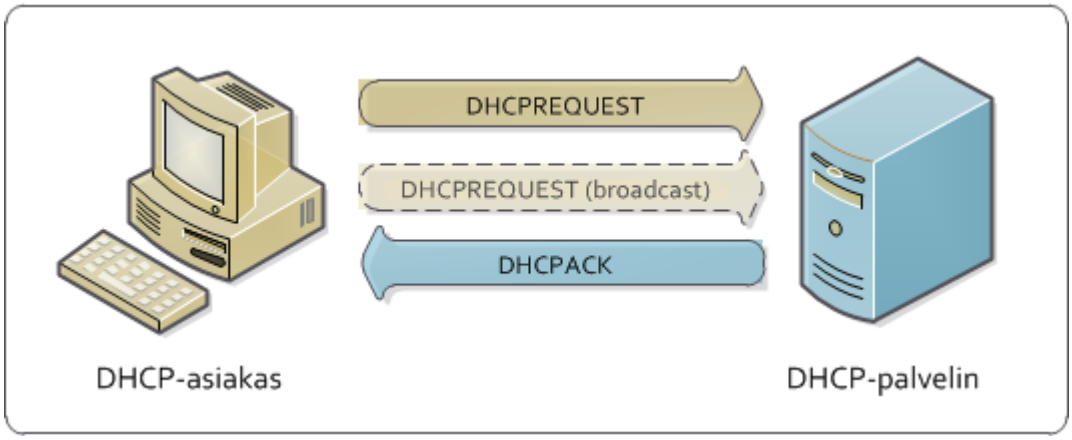


Kuva 6. DHCP-viestintä ensimmäisellä kerralla.

1. Kun asiakas käynnistyy tai liitetään verkkoon, se muodostaa DHCPDISCOVER viestejä ja lähettää niitä verkkoon löytääkseen palvelimen. Tässä vaiheessa asiakaslaitteella ei ole IP-osoitetta.
2. Kaikki viestin vastaanottaneet palvelimet muodostavat oman DHCPOFFER viestin, joka sisältää IP-osoitteen ja muut palvelimen tarjoamat asetukset. Viestit lähetetään asiakkaalle, joka voi saada niitä useammalta palvelimelta.
3. Ennalta määrätyn ajan kuluttua asiakaslaite lopettaa DHCPDISCOVER viestien lähettämisen ja valitsee yhden sille tarjotuista IP-osoitteista. Asiakas muodostaa DHCPREQUEST viestejä, jotka sisältävät valitun IP-osoitteen ja sitä tarjonneen palvelimen IP-osoitteen. Asiakas lähettää viestejä verkkoon, jolloin palvelimet tunnistavat tarjouksensa tulleen valituksi tai hylätyksi.
4. Kun valittu palvelin vastaanottaa DHCPREQUEST viestin, se lisää asiakkaalle tarjotun IP-osoitteen ja muut asetukset tietokantaansa. Palvelin käyttää tapahtuman yksilöllisenä tunnuksena asiakaslaitteen MAC-osoitetta (Media Access Control) ja sille jaettua IP-osoitetta.
5. Palvelin lähettää asiakkaalle DHCPACK viestin merkiksi tapahtuman onnistumisesta. Jos tapahtuma ei onnistunut, palvelin lähettää DHCPNACK viestin ja prosessi alkaa alusta.
6. Varmistaakseen ettei saatu IP-osoite ole käytössä toisella laitteella, asiakaslaite lähettää sen verkkoon käyttäen ARP-protokollaa (Address Resolution Protocol). Jos asiakaslaite ei saa vastausta, on prosessi valmis. Jos vastaus tulee, asiakaslaite hylkää saamansa IP-osoitteen ja aloittaa prosessin alusta.

Asetusten uusiminen

Kuvassa 2 on havainnollistettu protokollan mukaisia viestejä tilanteessa, jossa asiakas uusii laina-ajalla varustettuja asetuksiaan. Prosessi käsittää seuraavat kolme vaihetta:



Kuva 7. DHCP-viestintä lainan uusimiseksi.

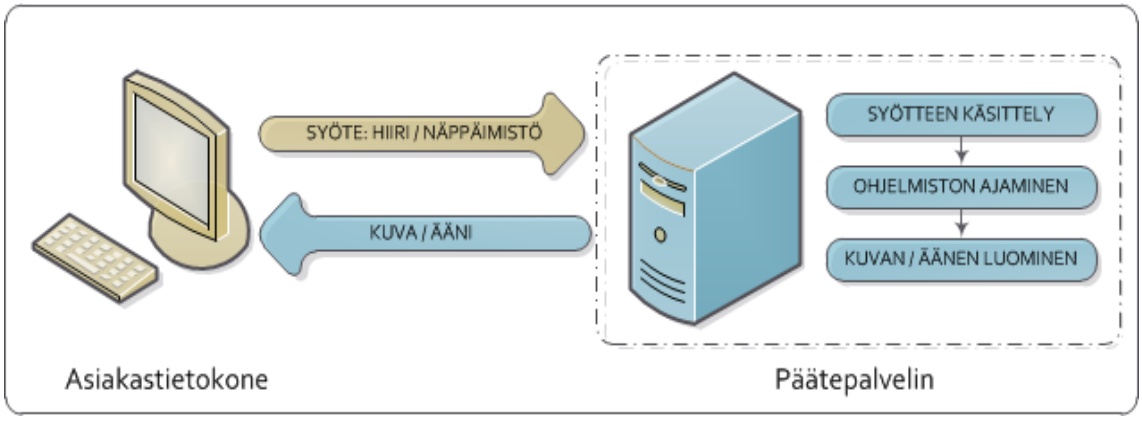
1. Kun laina-ajasta on kulunut 50 %, asiakas alkaa muodostaa DHCPREQUEST viestejä ja lähettämään niitä sille palvelimelle, jolta nykyinen laina on saatu. Asiakas uusii lainansa myös aina kun se käynnistyy.
2. Jos kyseinen palvelin ei vastaa ennen kuin asiakkaan laina-ajasta on kulunut 87,5 %, asiakas alkaa lähettämään DHCPREQUEST viestejä broadcast-muodossa, jolloin ne ovat kaikkien verkon laitteiden havaittavissa. Tällä toiminnalla asiakas yrittää saada asetukset miltä tahansa palvelimelta.
3. Jos alkuperäisen lainan myöntänyt palvelin vastaanottaa asiakkaan viestin, se voi vastata DHCPACK -viestillä, hyväksyen lainan uusimisen, tai DHCPNACK -viestillä, joka päättää lainan. Jos asiakas ei saa vastausta viesteihinsä laina-ajan loppuun mennessä, se vapauttaa nykyiset asetuksensa ja aloittaa uusien hankkimisen aikaisemmin selostetulla, 6-vaiheisella prosessilla. [6, s. 49-50; 11, s. 601; 14.]

5.3 Etätyöpöytäpalvelut

Etätyöpöytäpalvelu (Remote Desktop Services, RDS) on palvelinkäyttöjärjestelmään asennettava rooli sekä yleisnimitys sen sisältämille päätepalveluille. Päätepalveluilla tarkoitetaan niitä palvelimen toimintoja, joiden avulla asiakassovellusten suorittaminen, tietojen käsittely ja tallentaminen tapahtuvat palvelimessa ja niitä hyödynnetään asiakaslaitteilla. Palvelinta kutsutaan tällöin päätepalvelimeksi.

Asiakasohjelma lähettää palvelimelle näppäinpainalluksia ja hiiren liikuttamista koskevat tiedot. Palvelin käsittelee tiedot, suorittaa ohjelmistoa niiden mukaisesti ja

palauttaa asiakasohjelmalle tiedon siitä, mitä näytöllä tapahtuu. Etätyöpöydän ideaa on havainnollistettu kuvassa 3.



Kuva 8. Etätyöpöydän toimintaperiaate.

Asiakasohjelma

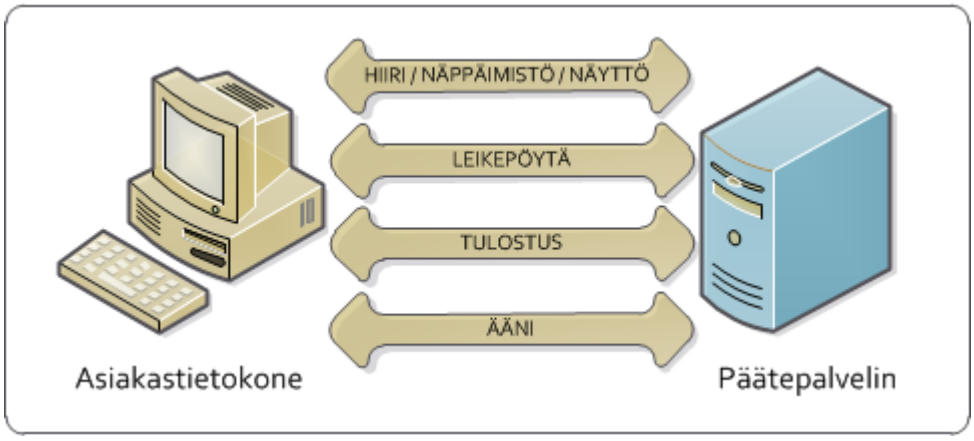
Päätepalveluita käytetään asiakasohjelman (Remote Desktop Connection, RDC) avulla, joka yhdistää palvelimeen ja todentaa käyttäjätunnuksen. Koska kaikki suoritettavien ohjelmistojen edellyttämä prosessointi tapahtuu palvelimella, ei asiakastietokoneen tarvitse täyttää niiden laitteistovaatimuksia. Asiakastietokoneelle riittää käyttöjärjestelmän ja asiakasohjelman suorittaminen, minkä ansiosta vaativiakin ohjelmistoja voidaan käyttää myös vanhemmilla tietokoneilla.

Etätyöpöytäyhteys päätepalvelimeen näkyy asiakasohjelmalla asetuksista riippuen joko palvelimen täydellisenä työpöytänä, vain yhden sovelluksen sisältävänä työpöytänä, tai yhtenä sovelluksena omassa ikkunassaan. Palvelimen täydellisen työpöydän käytön mahdollistavaa yhteyttä kutsutaan konsoliyhteydeksi.

Protokolla

Etätyöpöytäprotokolla (Remote Desktop Protocol, RDP) on Microsoftin kehittämä protokolla, joka mahdollistaa monikanavaisen siirron asiakasohjelman ja päätepalvelimen välillä. Monikanavaisuus tarkoittaa protokollan tapaa erotella etätyöpöytäyhteyden sisältö loogisiin osiin, joita kutsutaan kanaviksi.

Protokolla tukee 64 000 kanavaa, mutta vain pieni osa niistä on käytössä. Protokolla käyttää virtuaalisia kanavia, mikä mahdollistaa uusien, laitteiden välistä kommunikointia edellyttävien ominaisuuksien kehittämisen uusiin ja olemassa oleviin sovelluksiin. Kanavien sisältöä on havainnollistettu kuvassa 4.



Kuva 9. Protokollan määrittelemiä kanavia.

Aktiivisen etätyöpöytäyhteyden aikana asiakasohjelma päivittää näyttöä noin 20 kertaa sekunnissa. Kun yhteyttä ei aktiivisesti käytetä, laskee asiakasohjelma päivitysnopeuden 10 kertaan sekunnissa. Koska graafisen näyttötiedon välittäminen 10-20 kertaa sekunnissa aiheuttaa hyvin suuria tietomääriä, on protokollaan kehitetty useita kaistanleveyttä pienentäviä mekanismeja, kuten tiedon pakkaaminen ja välimuistin hyödyntäminen. Protokolla tallentaa asiakastietokoneen välimuistiin sellaiset elementit näytöllä, jotka eivät muutu päivitysten välillä. Näin päätepalvelimen tarvitsee lähettää ainoastaan muuttunut tieto, mikä vähentää huomattavasti siirrettävää tietomäärää.

Istunnot

Istunto (session) on kokoelma prosesseja, jotka muodostavat palvelimelle yksittäisen käyttäjäympäristön etätyöpöytäyhteyksiä varten. Päätepalvelin pystyy palvelemaan useita istuntoja samanaikaisesti. Kun useampi käyttäjä muodostaa palvelimelle etätyöpöytäyhteyden, on jokaisella käyttäjällä oma istuntonsa. Näin jokaisella käyttäjällä on oma työpöytä ja käyttäjäasetukset, jotka ovat täysin erillään muista istunnoista ja käyttäjistä. Istuntojen prosessit ovat erillään jopa tilanteessa, jossa samaa sovellusta käyttää useampi käyttäjä. Jos käyttäjä ajaa useampaa etäohjelmaa

(RemoteApp) samalla palvelimella, niin kyseiset etäohjelmat jakavat saman istunnon säästäen näin palvelimen resursseja.

Istuntojen pitämiseksi erillään palvelin antaa jokaiselle istunnolle uniikin tunnisteen. Istuntotunnisteet (Session ID) ovat lukuja, joiden jakamisen palvelin aloittaa 1:stä. Luku 0 on aina varattu järjestelmäpalveluille, mikä turvallisuussyistä erottaa ne sovelluksista. Kun päätepalvelu käynnistyy, se luo aina kaksi istuntoa valmiiksi etätyöpöytäyhteyksiä varten. Kun palvelimeen muodostetaan etätyöpöytäyhteys, se luo uuden istunnon odottamaan seuraavaa yhteyttä. Näin palvelin on aina valmiina vastaanottamaan yhteyksiä ja palvelemaan niitä mahdollisimman nopeasti.

Resurssien käyttö

Erillisistä istunnoista huolimatta, palvelimeen yhdistäneet käyttäjät jakavat yksittäisen palvelimen laitteisto- ja ohjelmistoresurssit. Erityisesti sovellusten suorittaminen on haaste, sillä ne eivät yleensä mahdollista osiensa erottelemista sessioille.

Esimerkiksi tekstinkirjoitusohjelman lataaminen kokonaan usealle käyttäjälle vaatisi suuren määrän muistia, ilman varsinaista hyötyä. Suurin osa ohjelman tiedostoista pysyy muuttumattomana sen käytön aikana, joten jakaminen käyttäjien kesken olisi huomattavasti tehokkaampaa. Ongelmaksi muodostuvat kuitenkin ne tiedostot, jotka muuttuvat. Yhden käyttäjän muuttaessa tiedoston sisältöä, välittyisi muutokset kyseiseen tiedostoon myös muille käyttäjille, joka aiheuttaisi ristiriitoja. Näin ei kuitenkaan käytännössä tapahdu, sillä palvelin käyttää muistinhallintamenetelmää, joka luo muokattavasta tiedostosta kopion kyseiselle sessiolle ja tekee muutokset siihen. Tämä minimoi muistin käytön per käyttäjä, ja mahdollistaa sovelluksen suorittamisen normaalisti. Näin myös tiedostot säilyvät erillään sessioiden välillä.

Lisenssit

Päätepalvelimeen yhdistävillä laitteilla ja käyttäjillä täytyy olla siihen oikeuttava lisenssi. Lisenssi on dokumentti, joka myöntää yksittäiselle laitteelle tai käyttäjälle pääsyn tiettyyn ohjelmistoon, joka on tässä tapauksessa päätepalvelu. Lisenssit on ostettava erikseen ja niiden käyttöönottoa ja hallintaa varten on asennettava lisenssipalvelin.

Etätyöpöytäpalvelu käsittää kaksi lisenssityyppiä: laitelisenssi ja käyttäjälisenssi. Laitelisenssi sallii pääsyn yhdelle laitteelle, riippumatta sen käyttäjästä. Käyttäjälisenssi sallii pääsyn yhdelle käyttäjälle, riippumatta miltä laitteelta käyttäjä muodostaa yhteyden.

Etätyöpöytäpalveluun sisältyy 120:n päivän vapaajakso, jonka aikana lisenssejä ei tarvita. Vapaajakson päätyttyä päätepalvelin ei enää hyväksy etätyöpöytäyhteyksiä, joille lisenssipalvelin ei ole myöntänyt lisenssejä.

Palvelimen etähallinnan mahdollistamiseksi käyttöjärjestelmä tukee konsoliyhteyksiä kahdelle käyttäjälle ilman, että käyttöjärjestelmään on asennettu etätyöpöytäpalveluiden rooli. Tällä tuella ei ole rajoituksia, eikä se vaadi lisenssejä.

Päätepalvelut

Palvelimelle asennettava etätyöpöytäpalveluiden rooli mahdollistaa päätepalvelimena toimimisen. Kyseiseen rooliin sisältyy seuraavat kuusi roolipalvelua:

RD Connection Broker mahdollistaa kuormituksen tasauksen usean päätepalvelimen kesken. RD Connection Broker tallentaa tilatiedot istunnoista, mikä mahdollistaa uudelleenyhdistämisen olemassa olevaan istuntoon.

RD Gateway mahdollistaa organisaation sisäisessä verkossa olevan päätepalvelimen käyttämisen internetin kautta. RD Gateway tunneloi etätyöpöytäliikenteen palomuurin tai NAT-laitteen (Network Address Translation) läpi käyttäen HTTPS-paketteja (Secure Hypertext Transfer Protocol).

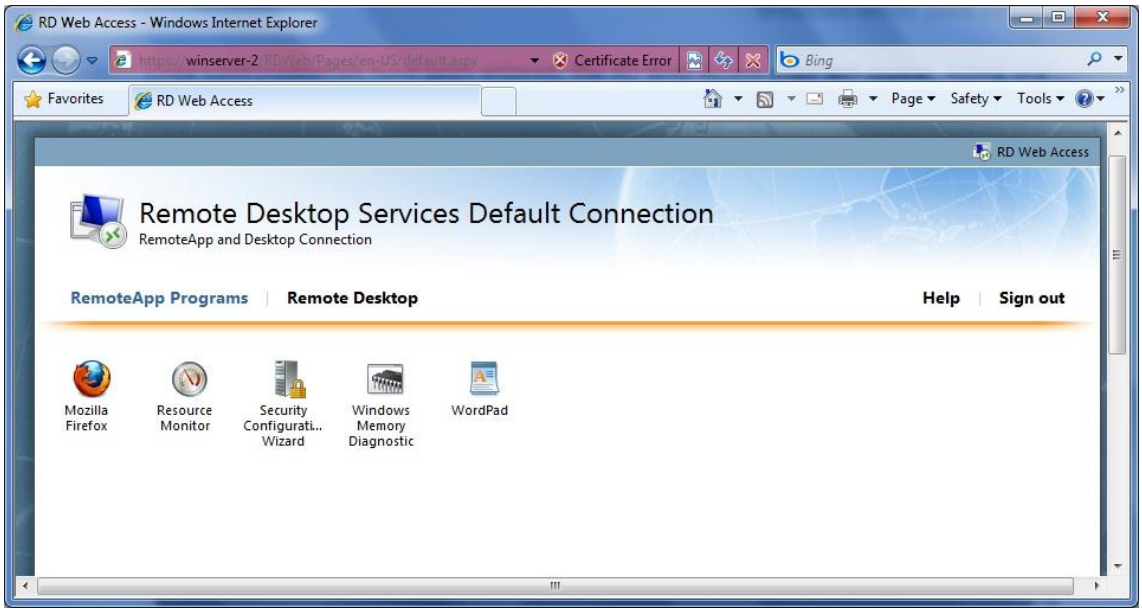
RD Licensing -palvelun asennuksella luodaan lisenssipalvelin, joka hallinnoi päätepalvelimeen yhdistävien laitteiden ja käyttäjien lisenssejä. Lisenssipalvelin sijaitsee siinä verkossa, jossa päätepalvelut ovat käytössä. Lisenssipalvelin voidaan asentaa samaan palvelimeen muiden päätepalveluiden kanssa.

RD Session Host käsittää päätepalvelimen perustoiminnot. RD Session Host tarjoaa palvelimeen yhdistävälle käyttäjälle mahdollisuuden käyttää kaikkia palvelimen

resursseja, kuten asennettuja sovelluksia. Palvelimen resurssien käyttöön on seuraavat kaksi toteutusta:

- Konsoliyhteys: Palvelimen työpöytä kaikkine ominaisuuksineen on käytettävissä asiakastietokoneelta.
- Etäohjelma (RemoteApp): Mahdollistaa palvelimelle asennetun sovelluksen ajamisen omassa ikkunassaan, aivan kuin se olisi asennettu asiakastietokoneelle paikallisesti. Etäohjelmat jaetaan käyttöön niistä luoduilla asennustiedostoilla tai RD Web Accessin kautta.

RD Web Access on palvelimen muodostama web-sivu, jonka käyttäjät voivat avata web-selaimella. Web-sivulta käyttäjät voivat avata konsoliyhteyden palvelimelle tai ajaa sen tarjoamia etäohjelmia. Näin käyttäjä ei tarvitse erillistä asiakasohjelmaa. Web-sivu voi olla käytettävissä internetissä tai vain organisaation sisäisessä verkossa. Kuvassa 10 on esimerkki web-sivusta, jonka kautta jaetaan etäohjelmia.



Kuva 10. Etäohjelmia käytettävissä RD Web Accessin kautta [15].

RD Virtualization Host on Hyper-V-virtualisointiympäristön ominaisuus, jolla Hyper-V voi hallita virtuaalikoneita ja tarjota ne käyttäjille virtuaalityöpöytinä. Jokaiselle käyttäjälle voidaan tarjota yksilöllinen työpöytä, tai voidaan tarjota työpöytien varanto.

Hyödyt

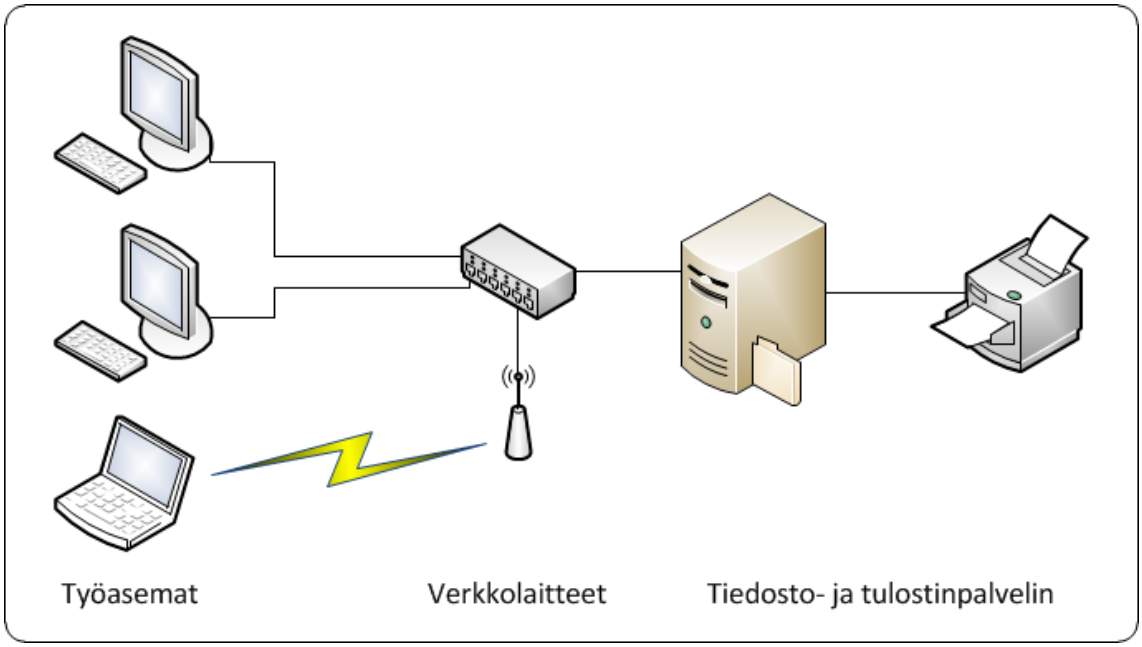
Etätyöpöytäpalveluiden käyttäminen tarjoaa useita hyötyjä organisaation tietotekniikalle, esimerkiksi paremman käytettävyyden ja taloudellisten säästöjen muodossa. Nämä palvelut myös helpottavat huomattavasti organisaation tietotekniikasta vastaavan henkilöstön töitä. Hyötyjä ovat muun muassa seuraavat asiat:

- Asiakaslaitteiden pienemmät laitteistovaatimukset: asiakastietokoneiden tarvitsee ajaa vain asiakasohjelmaa, mikä minimoi laitteistovaatimukset. Tämä mahdollistaa halvempien tietokoneiden ostamisen käyttäjille ja vähentää niiden laitteiston päivitystarvetta.
- Ohjelmistojen yksinkertaisempi jakelu, määrittäminen ja päivittäminen: ohjelmistoja ei tarvitse asentaa ja muokata jokaisella tietokoneella, vaan palvelimilla asentaminen ja muokkaaminen riittävät.
- Verkon kaistanleveyden pienempi käyttö: etätyöpöytäpalvelut käyttävät suhteellisen vähän kaistaa, koska suurin osa palvelimien ja asiakaslaitteiden välillä liikkuvasta tiedosta on syöttölaite- ja näyttötietoa. Myös yhteydet internetin kautta käyttävät huomattavasti vähemmän kaistaa kuin esimerkiksi VPN-yhteydellä (Virtual Private Network).
- Lisenssien tehokkaampi käyttö: lisenssiä ei tarvitse ostaa jokaiselle työasemalle, jolla ohjelmistoa saatetaan käyttää. Sen sijaan lisenssejä ostetaan tarpeellinen määrä palvelimelle, joka myöntää niitä sitä mukaan, kun käyttäjä ohjelmistoa oikeasti tarvitsee.
- Varmuuskopioinnin vähäisempi tarve: kun ohjelmistot ja tiedot sijaitsevat palvelimilla, ei asiakaslaitteita tarvitse varmuuskopioida kokonaan.
- Tuki ja koulutus etäyhteydellä: tukihenkilöstö voi käyttäjän luvalla liittyä käyttäjän istuntoon ja siten avustaa tehokkaasti ilman, että heidän tarvitsee olla toistensa luona fyysisesti.

Etätyöpöytäpalveluiden hyöty riippuu kuitenkin paljon laitteistosta, johon sen käyttöönottoa suunnitellaan. Jos esimerkiksi organisaatiossa on ostettu kalliit ja tehokkaat työasemat, ei ole järkeä käyttää niitä pelkästään asiakasohjelman ajamiseen. Jos kuitenkin laitteisto on vanhaa, etätyöpöytäpalvelu voi olla hyvin toimintakykyinen ja taloudellinen vaihtoehto laitteiston päivittämiselle tai uusimiselle. [6, s. 141-149; 11, s. 1023-1025; 16.]

5.4 Tiedosto- ja tulostinpalvelin

Yleisin palvelintyyppi organisaatioiden sisällä on tiedosto- ja tulostinpalvelin, joka mahdollistaa tiedostojen ja tulostimien järkevän jakamisen ja hallinnan organisaation sisäisessä verkossa. Tämä tarkoittaa tiedostojen ja tulostimien keskittämistä palvelimille, minkä avulla niitä voidaan käyttää useilta työasemilta ja hallita helpommin. Tiedosto ja –tulostinpalvelimena voi toimia vaikka tavallinen Windows-työasematietokone, mutta laitteistovaatimusten takia käytetään useimmiten erillistä palvelinta. Tiedostojen ja tulostimien keskittämistä on havainnollistettu kuvassa 11.



Kuva 11. Tiedostot ja tulostin jaetaan palvelimen avulla.

Windows Server 2008 R2 –käyttöjärjestelmässä perustiedosto- ja tulostinpalvelinominaisuudet ovat käytössä oletuksena, mutta niiden lisäksi molemmista palveluista on asennettavissa oma palvelinroolinsa.

Tiedostopalvelurooli tarjoaa tuen ja hallintakonsolit edistyneemmille tekniikoille, kuten hajautettu tiedostojärjestelmä (Distributed File System, DFS) ja verkkotiedostojärjestelmä (Network File System, NFS).

Tulostinpalvelurooli tarjoaa tuen UNIX-pohjaisille, LPR-tekniikkaa (Line Printer Remote) käyttäville asiakaslaitteille ja tulostustöiden vastaanoton niille luodun internetsivun kautta. [17, s. 106; 6, s. 199.]

Tiedostot

Tiedostojen jakaminen käyttäjien välillä ilman tiedostopalvelinta vaatisi työasemien kiintolevyjen jakamista ja niiden käyttöoikeuksien myöntämistä kaikille. Tämä kuitenkin johtaisi ennen pitkään kadonneisiin tiedostoihin, korruptoituneisiin työasemiin ja jatkuviin tukipyyntöihin työasemien käyttäjiltä.

Tiedostojen jakaminen palvelimella työasemien sijaan on suositeltavaa muun muassa seuraavista syistä:

- Tiedostojen jakaminen helpottuu.
- Varmuuskopiointi helpottuu.
- Käyttöoikeuksien määrittäminen helpottuu.
- Työasemien sisältöä ei tarvitse jakaa.
- Tiedostojakoja tarvitaan vähemmän.
- Tiedostojen käyttöä voidaan seurata ja levytilaa säätää sen perusteella.
- Käyttöoikeuksien ja tiedostojakojen määrittäminen ei näy käyttäjille. [6, s. 160-161.]

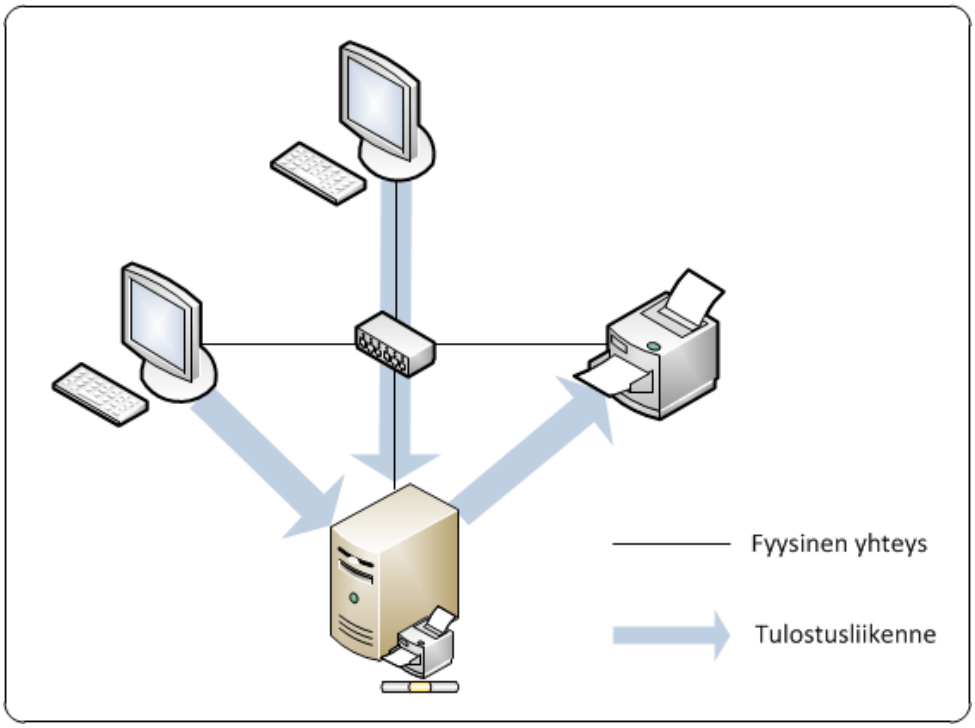
Tulostimet

Tulostin tai tulostimet voivat olla kytkettynä tulostinpalvelimeen ja sen kautta verkon työasemien käytettävissä, kuten kuvassa 11. Tulostimet voidaan myös kytkeä suoraan verkkoon, jos tulostinlaite sen mahdollistaa. Tällaista laitetta kutsutaan verkkotulostimeksi. Verkkotulostinta käytettäessä tulostinpalvelin ei ole välttämätön, koska jokainen työasema tai muu asiakaslaite voi lähettää tulostustyöt verkon läpi suoraan tulostimelle. Tällä toteutuksella on kuitenkin useita seuraavat haittapuolet:

- Käyttäjät näkevät tulostusjonossa vain omat tulostustyönsä, eivätkä siten tiedä koska tulostin vapautuu.
- Tulostusjonoa ei voida hallita keskitetysti, koska jokaisella laitteella on oma jononsa.

- Edistyneitä toimintoja, kuten tulostinvarantoa ja etähallintaa, ei voida käyttää.
- Virheviestit näkyvät vain sillä laitteella, josta tulostustyö on peräisin.
- Kaikki tulostustöiden käsittely tehdään työasemilla sen sijaan, että osa käsittelystä siirrettäisiin tulostinpalvelin suoritettavaksi.

Kaikki edellä mainitut haittapuolet voidaan kääntää eduksi käyttämällä tulostinpalvelinta myös verkkotulostimelle. Tätä toteutusta on havainnollistettu kuvassa 12. [6, s. 195-199.]



Kuva 12. Tulostinpalvelinta voidaan käyttää myös verkkotulostimen kanssa.

5.5 Web-palvelin

Web-palvelin tarkoittaa tietokonetta tai ohjelmistoa, joka vastaa asiakasohjelmien ja –laitteiden HTTP-protokollan mukaisiin palvelupyyntöihin. Web-palvelin vastaanottaa palvelupyyntöjä TCP/IP-verkosta, joka voi olla internet tai esimerkiksi yrityksen sisäinen verkko. Palvelupyynnön kohteena voi olla mikä tahansa tiedosto, mutta useimmiten kyseessä on HTML-tiedosto, jonka web-selain näyttää asiakaslaitteessa web-sivuna. Web-sivut voivat sisältää tekstiä, kuvia, ääntä, videota ja sovelluksia.

Windows Server 2008 -käyttöjärjestelmässä web-palvelimen toiminnallisuus saadaan asentamalla Web Server (IIS) -rooli. IIS (Internet Information Services) on Microsoftin kehittämä web-palvelinohjelmisto ja kyseisen web-palvelinroolin runko. IIS mahdollistaa web-palvelimen perustoiminnot, kuten web-sivun julkaisemisen. IIS sisältää lisäksi myös laajan valikoiman roolipalveluja erilaisten web-sovellusten toteuttamista, hallitsemista, diagnoimista ja turvaamista varten. Käyttöjärjestelmän sisältämän IIS:n versio on 7.0. [6, s. 131-133; 18, s. 20-21.]

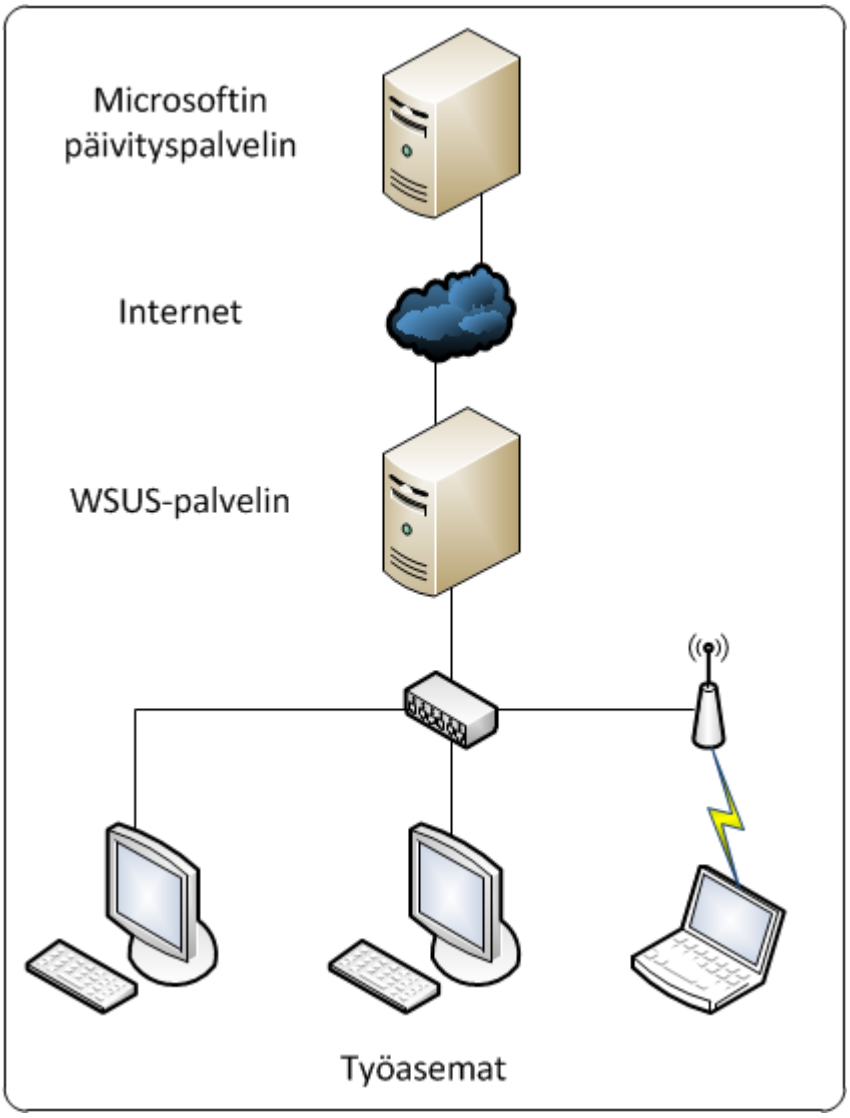
5.6 WSUS-palvelin

WSUS (Windows Server Update Services) on palvelinohjelmisto, joka lataa Windows-käyttöjärjestelmien päivitykset Microsoftin palvelimilta ja tallentaa ne WSUS-palvelimeen niiden arviointia ja jakelua varten.

WSUS-palvelimen käytön suurin etu on internet-yhteyden pienempi kuormitus, koska päivitykset tarvitsee ladata vain kerran. Jos esimerkiksi kaikki yrityksen tietokoneet lataisivat päivitykset itsenäisesti, voisi internetyhteyden kuormitus kasvaa valtavaksi, koska tietokoneita voi olla lukuisia ja päivitykset voivat olla suurikokoisia.

Toinen etu on järjestelmänvalvojan mahdollisuus arvioida ladatut päivitykset ja päättää niiden asentamisesta. Päivityksiin liittyy aina riski, että ne aiheuttavat ongelmia ja siksi niitä voidaan esimerkiksi kokeilla testiympäristössä, ennen kuin päätetään niiden asentamisesta.

Yksinkertaisin toteutus on käyttää yhtä WSUS-palvelinta, jolta asiakaslaitteet lataavat tarvitsemansa päivitykset. Tätä toteutusmallia on havainnollistettu kuvassa 13. Yksi WSUS-palvelin voi palvella jopa 25 000:tta asiakaslaitetta, joten se sopii useimpiin yritysverkkoihin.



Kuva 13. Yhden WSUS-palvelimen toteutusmalli.

Muita toteutusmalleja ovat usean WSUS-palvelimen käyttö itsenäisesti, synkronoidusti ja irti kytkettyinä. Itsenäisten palvelimien mallissa useat WSUS-palvelimet lataavat päivitykset internetistä ja jakavat niitä asiakaslaitteille, esimerkiksi kukin omassa lähiverkossaan. Synkronoidussa mallissa yksi WSUS-palvelin lataa päivitykset internetistä ja jakaa ne muille saman organisaation WSUS-palvelimille. Irti kytketty malli on sama kuin synkronoitu sillä erotuksella, että internetiin liitetyltä palvelimelta päivitykset siirretään muille palvelimille esimerkiksi ulkoisella kiintolevyllä.

Windows Server 2008 -käyttöjärjestelmässä WSUS-toiminnallisuuden asentaminen vaatii WSUS 3.0 SP1 -version tai uudemman. WSUS on ladattavissa ilmaiseksi

Microsoftin internet-sivuilta. Asennus vaatii myös Web Server (IIS) -roolin asennuksen ja Microsoft Report Viewer -ohjelman version 2005 tai uudemman. [6, s. 411-414.]

6 Toteutus

6.1 Laitteisto

Komponentit

Palvelinlaitteistoksi päätettiin hankkia uusi ja suhteellisen monipuolinen kokonaisuus, jotta se täyttäisi luvussa 2.2 luetellut vaatimukset esimerkiksi luotettavuuden ja laajennettavuuden osalta. Komponentit valittiin tunnetuilta valmistajilta ja hankittiin tunnetuilta, kotimaisilta yrityksiltä. Kiintolevykelkat hankittiin EET:ltä ja kaikki loput komponentit Verkkokauppa.comista. Taulukossa 1 on listattu kaikki hankitut komponentit, mukaan lukien käyttöjärjestelmä.

Taulukko 1. Hankittu palvelinlaitteisto ja -ohjelmisto.

Komponentti	Valmistaja ja malli	Lukumäärä	Hinta € (ALV 0% | 23%)	
Palvelin	HP ProLiant ML350 G6 Xeon E5606/1x4GiB/6LFF 5U	1	1300,7	1599,9
Lisämuistikampa	Kingston 4GiB DDR3 1066MHz Quad Rank LP ECC REG	1	61,7	75,9
Käyttöjärjestelmä	Microsoft Windows Server 2008 R2 Standard	1	543,0	667,9
Varavirtalähde	HP ProLiant 460W Common Slot High Efficiency Gold 12V Hot Plug AC	1	182,0	223,9
Varatuuletinsarja	HP ProLiant ML350 G6 vikasietoinen tuuletinsarja	1	43,0	52,9
Kiintolevyt	Western Digital Caviar RE4 1TiB SA-TA2 7200RPM 64MB	2	151,1	185,8
Kiintolevykelkat	MicroStorage 3.5" SATA/SAS HotSwap Tray	2	69,5	85,5
Ulkoinen kovalevy	Western Digital Elements Desktop 1TiB USB 2.0 7200RPM	1	52,8	64,9
Näyttö	Acer P196HQVb 18.5" HD Ready LCD	1	73,1	89,9
Näppäimistö	Logitech Keyboard K120 for Business USB	1	8,9	10,9
Hiiri	Logitech B110 Optical USB Mouse	1	7,2	8,9
		Yhteensä:	**2493,0**	**3066,4**

Palvelimeksi valittiin Hewlett-Packardin valmis tornipalvelin, joka sisältää 4-ytimisen suorittimen, 4 GiB muistia, DVD-aseman ja perus RAID-tasoja tukevan kiintolevyohjaimen. Palvelin sisältää 6 kpl SAS/SATA-kiintolevypaikkoja LFF-kokoisille kiintolevyille. Palvelimessa on laajennusta varten paikat toiselle suorittimelle, yhteensä 18:sta muistikammalle ja 6:lle PCI Express -liitäntäiselle lisälaitteelle. Palvelimella on 36 kuukauden NBD (Next Business Day) on-site takuu, mikä tarkoittaa, että palvelimen vikaantuessa huoltohenkilö saapuu seuraavana työpäivänä korjaamaan sitä tai vaihtamaan sen.

Palvelimeen hankittiin samalla yksi 4 Gibitavun lisämuistikampa ja paikallista hallintaa varten edullinen näyttö, näppäimistö ja hiiri.

Vikasietoisuuden parantamiseksi palvelimeen hankittiin lisäksi ns. hot plug –toiminnallisuutta tukeva toinen virtalähde ja tuuletinsarja. Tämä mahdollistaa ensisijaisen virtalähteen ja tuulettimien hajoamisen ilman, että palvelimen toiminta keskeytyy. Myös kiintolevypaikat ja -liitännät mahdollistavat hot plug –toiminnallisuuden.

Kiintolevyiksi hankittiin 2 kpl 1 tibitavun kokoista Western Digital RE4 -mallia, jotka ovat erityisesti vaativaan yrityskäyttöön suunniteltuja. Kiintolevyt ovat SATA-liitäntäisiä. Kiintolevyjen asennusta varten jouduttiin hankkimaan myös erilliset kiintolevykelkat, joilla kiintolevyt liitetään palvelimeen ja jotka mahdollistavat niiden nopean irrottamisen ja asentamisen. Varmuuskopiointia varten hankittiin ulkoinen, USB-liitäntäinen kiintolevy. Ulkoinen kiintolevy on sisäisten tapaan Western Digitalin valmistama ja kapasiteetiltaan 1 TiB.

6.2 Käyttöjärjestelmä

Valintaperusteet

Palvelimen käyttöjärjestelmäksi valittiin Windows Server 2008 R2, joka on tällä hetkellä Windows Server -palvelinkäyttöjärjestelmän uusin versio. Päätös kyseisen käyttöjärjestelmän valinnasta tehtiin aivan alkuvaiheessa, jo huomattavasti ennen laitteiston valintaa.

Käyttöjärjestelmän valintaperusteista suurin oli oma aikaisempi kokemukseni, sillä olen opetellut ja käyttänyt kyseistä käyttöjärjestelmää koulussa useilla kursseilla. Tästä on huomattavasti hyötyä, koska palvelimeen liittyvät toimenpiteet asennuksesta käyttöönottoon ja ylläpitoon ovat vastuullani.

Toinen merkittävä valintaperuste oli palvelinkäyttöjärjestelmän yhteensopivuus yrityksen muiden ohjelmistojen ja muiden tietokoneiden kanssa, sillä ne kaikki käyttävät Windows-käyttöjärjestelmiä. Tämän ansiosta esimerkiksi etätyöpöytäpalveluiden käyttöönotto on suoraviivaista ja palvelimessa voidaan käyttää samaa tietoturvaohjelmistoa, kuin työasematietokoneissa.

Myös yrityksen henkilöstön aikaisemmat kokemukset Windows-käyttöjärjestelmistä vaikuttivat valintaan, koska palvelinkäyttöjärjestelmän rakenne ja graafinen käyttöliittymä on hyvin saman kaltainen kuin työasemaversioissa. Tämän ansiosta palvelimen hallinnan opettaminen tarvittaessa muille henkilöille on mielekästä.

Lisenssit

Hankittu käyttöjärjestelmäversio sisältää valmiina yhden palvelinlisenssin ja 5 käyttölisenssiä. Käyttölisenssit voi myöntää joko käyttäjä- tai laitekohtaisesti. Tämä tarkoittaa sitä, että käyttöjärjestelmää voi käyttää vain yhdellä palvelimella ja sitä voi käyttää enintään 5 käyttäjää tai laitetta. Kohdeyrityksen toteutuksessa nämä lisenssit riittävät toistaiseksi palvelimen sujuvaan hyödyntämiseen.

Käyttöjärjestelmä ei sisällä lisenssejä etätyöpöytäpalveluiden käyttöön, mutta se mahdollistaa 120 päivän kokeilujakson, jonka aikana lisenssejä ei tarvita. Kohdeyrityksen toteutuksessa palvelimella on tarkoitus suorittaa laskutusohjelmistoa ja mahdollistaa sen käyttö etätyöpöytäpalveluiden etäohjelma (RemoteApp) -toiminnallisuden avulla. Tästä johtuen etätyöpöytäpalveluiden lisenssejä tarvitaan, mutta kokeilujakson takia niiden hankkiminen on päätetty jättää myöhemmäksi. Näin etätyöpöytäpalveluita päästään kokeilemaan ja käyttämään, jolloin lisenssien lukumäärän ja tyypin todellinen tarve tulee ilmi ennen, kuin niitä tarvitsee vielä hankkia.

7 Yhteenveto

Insinöörityössä tutkittiin erilaisia palvelinlaitteistoja, niihin liittyviä teknologioita ja valitun Windows Server 2008 -käyttöjärjestelmän ominaisuuksia, konfigurointia ja hallintaa. Näiden tietojen tutkimisen tarkoituksena oli saavuttaa sellainen tietotaso, jonka perusteella osattaisiin suunnitella kohdeyrityksen tarpeisiin soveltuva palvelinratkaisu.

Tutkimustyön tuloksena oli pitkälle mietitty laitteistokokonaisuus ja suunnitelma siitä, mitä ja miten valitun laitteiston ja käyttöjärjestelmän mahdollistamia ominaisuuksia

tultaisiin käyttämään. Näiden perusteella suoritettiin tarvittavat laitteisto- ja ohjelmistohankinnat.

Suunnitellun palvelinratkaisun asennus, testaus ja käyttöönotto eivät sisältyneet tähän insinöörityöraporttiin, koska niiden ajankohta siirtyi myöhemmäksi laitteiston pitkän toimitusajan ja yrityksen toimitilojen vaihdon takia. Tästä johtuen raportti ei valitettavasti sisällä tietoa palvelinratkaisun toiminnasta käytännössä, mutta kyseiset toimenpiteet ovat edelleen osa palvelinratkaisun suunnittelua ja toteutusta, ja ne tullaan tähänastisen tutkimus- ja suunnittelutyön jatkona tekemään.

Lähteet

1 Tavu (tietotekniikka). 2011. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Tavu_(tietotekniikka)>. Päivitetty 1.6.2011. Luettu 30.8.2011.

2 rack dell server. 2011. Verkkodokumentti. Server Rack. <http://www.serverrack2.com/rack-dell-server/>. Luettu 24.8.2011.

3 Blade server. 2011. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Blade_server>. Päivitetty 9.8.2011. Luettu 24.8.2011.

4 Server (computing). 2011. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Server_(computing)>. Muokattu 15.8.2011. Luettu 21.9.2011.

5 Unbuffered versus Registered ECC Memory – Difference between ECC UDIMMs and RDIMMs. 2011. ServeTheHome. <http://www.servethehome.com/unbuffered-registered-ecc-memory-difference-ecc-udimms-rdimms/>. Luettu 21.9.2011.

6 Zacker, Craig. 2009. Windows Server 2008 Administrator. Hoboken: WILEY.

7 Investigation: Is Your SSD More Reliable Than A Hard Drive?. 2011. Verkkodokumentti. Tom's Hardware. <http://www.tomshardware.com/reviews/ssd-reliability-failure-rate,2923.html>. Luettu 19.9.2011.

8 Serial attached SCSI. 2011. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Serial_attached_SCSI>. Muokattu 29.8.2011. Luettu 19.9.2011.

9 RAID. 2011. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/RAID>. Päivitetty 28.8.2011. Luettu 30.8.2011.

10 Standard RAID levels. 2011. Verkkodokumentti. Wikipedia. < http://en.wikipedia.org/wiki/Standard_RAID_levels>. Päivitetty 28.8.2011. Luettu 30.8.2011.

11 Kivimäki, Jyrki. 2009. Windows Server 2008 R2 Tehokas hallinta. Hämeenlinna: readme.fi.

12 Windows NT. 2011. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Windows_NT>. Muokattu 19.8.2011. Luettu 20.10.2011.

13 Server Manager. 2008. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/cc732131(WS.10).aspx>. Muokattu 21.1.2008. Luettu 19.10.2011.

14 DHCP. 2011. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/DHCP>. Päivitetty 1.6.2011. Luettu 18.6.2011.

15 Configuring Windows Server 2008 RD Web Access. 2010. Verkkodokumentti. Techotopia.com. <http://www.techotopia.com/index.php/Configuring_Windows_Server_2008_RD_Web_Access>. Päivitetty 1.4.2011. Luettu 16.7.2011.

16 Remote Desktop Protocol. 2011. Verkkodokumentti. Microsoft. <http://msdn.microsoft.com/en-us/library/aa383015(v=vs.85).aspx>. Luettu 13.7.2011.

17 Zacker, Craig. 2009. Windows Server 2008 Applications Infrastructure Configuration. Hoboken: WILEY.

18 Kuosmanen, Harri. 2009. Windows Server 2008:n roolit ja asennus. Opinnäytetyö. Tampereen ammattikorkeakoulu.